

A Matrix Ring Description for Cyclic Convolutional Codes

Heide Gluesing-Luerssen*, Fai-Lung Tsang†

February 1, 2008

Abstract: In this paper, we study convolutional codes with a specific cyclic structure. By definition, these codes are left ideals in a certain skew polynomial ring. Using that the skew polynomial ring is isomorphic to a matrix ring we can describe the algebraic parameters of the codes in a more accessible way. We show that the existence of such codes with given algebraic parameters can be reduced to the solvability of a modified rook problem. It is our strong belief that the rook problem is always solvable, and we present solutions in particular cases.

Keywords: Convolutional codes, cyclic codes, skew polynomial rings, Forney indices.

MSC (2000): 94B10, 94B15, 16S36

1 Introduction

Convolutional codes (CC's, for short) form an important class of error-correcting codes in engineering practice. The mathematical theory of these codes has been set off by the seminal papers of Forney [3] and Massey et al. [15], and the progress ever since is reflected by, for instance, the books [12, 19] and the article [16]. Several directions have been pursued. In the 1970s, a lot of effort has been made to construct powerful CC's with the aid of good block codes, see [14, 13]. This idea has been resumed in the papers [24, 7]. Furthermore, the methods of linear systems theory have been utilized in order to gain a deeper mathematical understanding of CC's. We refer to the papers [15, 21, 23, 10] for further details and constructions. A third direction in the theory of CC's developed when codes with some additional algebraic structure were studied. Besides the recently introduced classes of Goppa convolutional codes [1, 17] and group convolutional codes [2], the main class of such codes are cyclic convolutional codes.

Cyclic structure for CC's has been investigated for the first time in the papers [18, 20]. One of the crucial observations revealed that CC's that are invariant under the ordinary cyclic shift have degree zero, that is, they are cyclic block codes. This insight has led to

*University of Kentucky, Department of Mathematics, 715 Patterson Office Tower, Lexington, KY 40506-0027, USA; heidegl@ms.uky.edu

†University of Groningen, Department of Mathematics, P. O. Box 800, 9700 AV Groningen, The Netherlands; F.L.Tsang@math.rug.nl

a more complex notion of cyclicity for CC's which can be summarized as follows. Cyclic convolutional codes (CCC's, for short) are direct summands of $\mathbb{F}[z]^n$ that are at the same time left ideals in a skew polynomial ring $A[z; \sigma]$, where $A = \mathbb{F}[x]/\langle x^n - 1 \rangle$ and σ is an \mathbb{F} -automorphism of A . During the last couple of years a detailed algebraic theory of CCC's has been developed in [8, 6]. Among other things it has been shown that CCC's are principal left ideals in $A[z; \sigma]$ and, using a type of Gröbner basis theory, one can compute reduced generator polynomials from which all algebraic parameters of the code can easily be read off. The details will be given later on in Theorem 3.5. Classes of CCC's with good error-correcting properties have been presented in [5, 9].

In this paper we want to continue the investigation of CCC's. We restrict ourselves to a particular class of automorphisms. In that case the skew polynomial ring $A[z; \sigma]$ turns out to be isomorphic to a matrix ring over a commutative polynomial ring. This allows us to easily construct generator polynomials of CCC's with prescribed algebraic parameters. Moreover, we discuss the existence of CCC's with any given algebraic parameters and will show that it reduces to a particular combinatorial problem resembling the classical rook problem. We can solve particular instances of that problem, but unfortunately not the general case. However, we strongly believe that the combinatorial problem is solvable for all possible cases.

The outline of the paper is as follows. In the next section we review important notions from convolutional coding theory and introduce the algebraic framework for CCC's. In Section 3 we concentrate on a particular class of CCC's and establish an isomorphism between the associated skew polynomial ring and a certain matrix ring. We translate the main notions needed for the theory of CCC's into the matrix setting. In Section 4 we construct particular CCC's and discuss the existence of CCC's with given Forney indices. The existence of such codes reduces to a combinatorial problem followed by a problem of constructing polynomial matrices with certain degree properties. After presenting a proof of the matrix problem we discuss and solve particular instances of the combinatorial problem in Section 5. We close the paper with a short section illustrating how to generalize the results to codes that are cyclic with respect to a general automorphism.

2 Preliminaries on Cyclic Convolutional Codes

Throughout this paper let \mathbb{F} be a finite field with q elements. A *convolutional code of length n and dimension k* is a submodule \mathcal{C} of $\mathbb{F}[z]^n$ having the form

$$\mathcal{C} = \text{im } G := \{uG \mid u \in \mathbb{F}[z]^k\},$$

where G is a *basic* matrix in $\mathbb{F}[z]^{k \times n}$, i. e. $\text{rank } G(\lambda) = k$ for all $\lambda \in \overline{\mathbb{F}}$ (with $\overline{\mathbb{F}}$ being an algebraic closure of \mathbb{F}). We call such a matrix G an *encoder*, and the number $\deg(\mathcal{C}) := \deg(G) := \max\{\deg(M) \mid M \text{ is a } k\text{-minor of } G\}$ is said to be the *degree* of the encoder G or of the code \mathcal{C} . Recall that the requirement of G being basic (rather than just having full row rank over $\mathbb{F}[z]$) is equivalent to \mathcal{C} being a direct summand of the module $\mathbb{F}[z]^n$. Obviously, two basic matrices $G, G' \in \mathbb{F}[z]^{k \times n}$ satisfy $\text{im } G = \text{im } G'$ if and only if $G' = UG$ for some $U \in GL_k(\mathbb{F}[z]) := \{V \in \mathbb{F}[z]^{k \times k} \mid \det(V) \in \mathbb{F} \setminus \{0\}\}$. It is well known [4, p. 495]

that each CC admits a minimal encoder. Here a matrix $G \in \mathbb{F}[z]^{k \times n}$ is said to be *minimal* if the sum of its row degrees equals $\deg(G)$, where the degree of a polynomial row vector is defined as the maximal degree of its entries. For details see, e. g., [4, Main Thm.] or [16, Thm. A.2]. Such a minimal encoder is in general not unique; the row degrees of a minimal encoder, however, are, up to ordering, uniquely determined by the code and are called the *Forney indices* of the code or of the encoder. It follows that a CC has a constant encoder matrix if and only if the degree is zero. In that case the code is, in a natural way, a block code.

Beyond these purely algebraic concepts the most important notion in error-control coding is certainly the weight. For a polynomial vector $v = \sum_{j=0}^N v^{(j)} z^j \in \mathbb{F}[z]^n$, where $v^{(j)} \in \mathbb{F}^n$, one defines its weight as $\text{wt}(v) = \sum_{j=0}^N \text{wt}(v^{(j)})$, with $\text{wt}(v^{(j)})$ denoting the (Hamming) weight of the vector $v^{(j)} \in \mathbb{F}^n$. Just like for block codes the *distance* of a code \mathcal{C} is defined as $\text{dist}(\mathcal{C}) = \min\{\text{wt}(v) \mid v \in \mathcal{C}, v \neq 0\}$.

Let us now turn to the notion of cyclicity (for details we refer to [8, 6]). We will restrict ourselves to codes where the length n is coprime with the field size q . From the theory of cyclic block codes recall the standard identification

$$\mathfrak{p} : \mathbb{F}^n \longrightarrow A := \mathbb{F}[x]/\langle x^n - 1 \rangle, \quad (v_0, \dots, v_{n-1}) \longmapsto \sum_{i=0}^{n-1} v_i x^i \quad (2.1)$$

of \mathbb{F}^n with the ring of polynomials modulo $x^n - 1$. Extending this map coefficientwise we can identify the polynomial module $\mathbb{F}[z]^n = \{\sum_{\nu=0}^N z^\nu v_\nu \mid N \in \mathbb{N}_0, v_\nu \in \mathbb{F}^n\}$ with the polynomial ring

$$A[z] := \left\{ \sum_{\nu=0}^N z^\nu a_\nu \mid N \in \mathbb{N}_0, a_\nu \in A \right\}.$$

Following the theory of cyclic block codes one would like to declare a code $\mathcal{C} \subseteq \mathbb{F}[z]^n$ cyclic if it is invariant under the cyclic shift acting on $\mathbb{F}[z]^n$, or, equivalently, if its image in $A[z]$ is an ideal. However, it has been shown in various versions in [18, Thm. 3.12], [20, Thm. 6], and [8, Prop. 2.7] that every CC with this property has degree zero. In other words, this notion does not lead to any codes other than cyclic block codes. Due to this result a more general notion of cyclicity has been introduced and discussed in the papers mentioned above. In order to present this notion we need the group $\text{Aut}_{\mathbb{F}}(A)$ of all \mathbb{F} -automorphisms on A . It is clear that each automorphism $\sigma \in \text{Aut}_{\mathbb{F}}(A)$ is uniquely determined by the single value $\sigma(x) \in A$, but not every choice for $\sigma(x)$ determines an automorphism on A . Indeed, since x generates the \mathbb{F} -algebra A the same has to be true for $\sigma(x)$, and we obtain for $a \in A$

$$\left. \begin{array}{l} \sigma(x) = a \text{ determines an} \\ \mathbb{F}\text{-automorphism on } A \end{array} \right\} \iff \left\{ \begin{array}{l} 1, a, \dots, a^{n-1} \text{ are linearly independent} \\ \text{over } \mathbb{F} \text{ and } a^n = 1. \end{array} \right. \quad (2.2)$$

Fixing an arbitrary automorphism $\sigma \in \text{Aut}_{\mathbb{F}}(A)$ we define a new multiplication on the $\mathbb{F}[z]$ -module $A[z]$ via

$$az = z\sigma(a) \text{ for all } a \in A. \quad (2.3)$$

Along with associativity, distributivity, and the usual multiplication inside A this turns $A[z]$ into a skew polynomial ring which we will denote by $A[z; \sigma]$. Notice that $A[z; \sigma]$ is

non-commutative unless σ is the identity. Moreover, the map \mathbf{p} from (2.1) can be extended to

$$\mathbf{p} : \mathbb{F}[z]^n \longrightarrow A[z; \sigma], \quad \sum_{\nu=0}^N z^\nu v_\nu \longmapsto \sum_{\nu=0}^N z^\nu \mathbf{p}(v_\nu), \quad (2.4)$$

this way yielding an isomorphism of left $\mathbb{F}[z]$ -modules. Now we declare a submodule $\mathcal{C} \subseteq \mathbb{F}[z]^n$ to be σ -cyclic if $\mathbf{p}(\mathcal{C})$ is a left ideal in $A[z; \sigma]$. It is straightforward to see that the latter is equivalent to the $\mathbb{F}[z]$ -submodule $\mathbf{p}(\mathcal{C})$ of $A[z; \sigma]$ being closed under left multiplication by x . Combining this with the definition of CC's we arrive at the following notion.

Definition 2.1 A submodule $\mathcal{C} \subseteq \mathbb{F}[z]^n$ is called a σ -cyclic convolutional code (σ -CCC, for short) if \mathcal{C} is a direct summand of $\mathbb{F}[z]^n$ and $\mathbf{p}(\mathcal{C})$ is a left ideal in $A[z; \sigma]$.

In the papers [18, 8, 6, 5, 9] the algebraic properties of these codes have been investigated in detail (the main results are summarized in Theorem 3.5 below) and plenty of CCC's, all optimal with respect to their free distance, have been presented. In [5] a class of one-dimensional CCC's has been constructed all of which members are MDS codes, that is, they have the best distance among all one-dimensional codes with the same length, same degree and over any finite field. This result has been generalized to a class of Reed-Solomon convolutional codes in [9]. In [2] the concept of cyclicity has been generalized to group convolutional codes.

Let us close this section with some basic notation. In any ring we will denote left, respectively right, ideals by $\bullet \langle \cdot \rangle$, respectively $\langle \cdot \rangle \bullet$. As usual, ideals in commutative rings will be written as $\langle \cdot \rangle$. The group of units in a ring R will be denoted by R^\times .

3 The Matrix Ring \mathcal{M}

In this paper we will restrict ourselves to a more specific class of cyclic codes than those being introduced in the previous section. Indeed, we will consider the following situation. Let \mathbb{F} be any field with q elements and let $n \in \mathbb{N}_{\geq 2}$ be a divisor of $q - 1$. Then, using the Chinese Remainder Theorem, the quotient ring $A' := \mathbb{F}[x]/\langle x^n - 1 \rangle$ is isomorphic to the direct product

$$A := \underbrace{\mathbb{F} \times \cdots \times \mathbb{F}}_{n \text{ copies}}. \quad (3.1)$$

The elements of A will be denoted as $a = [a_1, \dots, a_n]$, where $a_i \in \mathbb{F}$ for $i = 1, \dots, n$. Observe that \mathbb{F} naturally embeds into A via $f \longmapsto [f, \dots, f]$, thus A is an \mathbb{F} -algebra. This algebra structure is isomorphic to the natural \mathbb{F} -algebra structure of A' .

The standard \mathbb{F} -basis of A is given by $\{e_1, \dots, e_n\}$, where

$$e_i = [0, \dots, 1, \dots, 0] \text{ with the } 1 \text{ appearing in the } i\text{-th position.} \quad (3.2)$$

Obviously, these are just the primitive idempotents of the ring A , and $A = \bigoplus_{i=1}^n \langle e_i \rangle$ as a direct sum of ideals. It is clear that the automorphisms of A are in one-one correspondence

with the permutations of the primitive idempotents. As a consequence, $|\text{Aut}_{\mathbb{F}}(A)| = n!$, see also [8, Cor. 3.2]. In this paper, we will consider only those automorphisms for which the permutation is a cycle of length n . It is not hard to see that there are exactly $(n-1)!$ automorphisms of that kind. Allowing a suitable permutation of the n copies of \mathbb{F} , we may restrict ourselves to the automorphism

$$\sigma : A \longrightarrow A, \quad \sigma([a_1, \dots, a_n]) = [a_n, a_1, \dots, a_{n-1}]. \quad (3.3)$$

Then $\sigma(e_i) = e_{i+1}$ for $1 \leq i \leq n-1$ and $\sigma(e_n) = e_1$, and we have the identities

$$\sigma^j(e_i) = e_{(i+j-1 \bmod n)+1} \text{ for all } i = 1, \dots, n \text{ and } j \in \mathbb{N}_0. \quad (3.4)$$

As in the previous section, the automorphism σ gives rise to a skew polynomial ring $(A[z; \sigma], +, \cdot)$ where, again, the set $\{\sum_{\nu=0}^N z^\nu a_\nu \mid N \in \mathbb{N}_0, a_\nu \in A\}$ is equipped with the usual coordinatewise addition, and where multiplication is defined by the rule $az = z\sigma(a)$ for all $a \in A$, see (2.3). As already indicated by the notation above, coefficients of the polynomials in $A[z; \sigma]$ are always meant to be the right hand side coefficients. Again, the left $\mathbb{F}[z]$ -module $A[z; \sigma]$ is isomorphic to $\mathbb{F}[z]^n$ via the map \mathfrak{p} from (2.4), and where we use an isomorphism of A with the quotient ring A' . Thus, $A[z; \sigma]$ gives us the framework for the class of CCC's where the length n divides $q-1$ and where the underlying automorphism induces a cycle of length n on the primitive idempotents.

Example 3.1 Let $\mathbb{F} = \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, where $\alpha^2 = \alpha + 1$, and let $n = 3$. Then $A = \mathbb{F} \times \mathbb{F} \times \mathbb{F} \cong \mathbb{F}[x]/\langle x^3 - 1 \rangle = A'$ and $|\text{Aut}_{\mathbb{F}}(A)| = 6$. The automorphisms $\sigma \in \text{Aut}_{\mathbb{F}}(A')$ are completely determined by their value $\sigma(x)$ assigned to x , see also (2.2). These values are given by $x, x^2, \alpha x, \alpha^2 x, \alpha x^2, \alpha^2 x^2$. The two automorphisms inducing cycles of length 3 are given by $\sigma_1(x) = \alpha x$ and $\sigma_2(x) = \alpha^2 x$. Indeed, using the isomorphism $\phi : A' \longrightarrow A, f \longmapsto [f(1), f(\alpha), f(\alpha^2)]$ the primitive idempotents of A are $e_1 = [1, 0, 0] = \phi(x^2 + x + 1)$, $e_2 = [0, 1, 0] = \phi(\alpha x^2 + \alpha^2 x + 1)$, and $e_3 = [0, 0, 1] = \phi(\alpha^2 x^2 + \alpha x + 1)$. One easily verifies that $\sigma_2(e_1) = e_2$, $\sigma_2(e_2) = e_3$, $\sigma_2(e_3) = e_1$, thus σ_2 satisfies (3.3) (where, of course, we identify $\sigma_2 \in \text{Aut}_{\mathbb{F}}(A')$ with $\phi \sigma_2 \phi^{-1} \in \text{Aut}_{\mathbb{F}}(A)$). Likewise, using the identification $A' \longrightarrow A, f \longmapsto [f(\alpha^2), f(\alpha), f(1)]$ the automorphism σ_1 satisfies (3.3). Notice that $\sigma_2 = \sigma_1^{-1}$.

In the rest of this section we will show how the skew polynomial ring $A[z; \sigma]$ can be described as a certain matrix ring, and we will translate various properties into the matrix setting. This will lead us to a new way of constructing CCC's with given algebraic parameters. Let us consider the ring $\mathbb{F}[t]^{n \times n}$ of polynomial matrices in an indeterminate t and define the subset

$$\mathcal{M} := \{(m_{ab}) \in \mathbb{F}[t]^{n \times n} \mid m_{ab}(0) = 0 \text{ for all } 1 \leq b < a \leq n\}.$$

Notice that \mathcal{M} consists exactly of all matrices where the elements below the diagonal are multiples of t . It is easy to see that \mathcal{M} is a (non-commutative) subring of $\mathbb{F}[t]^{n \times n}$.

Proposition 3.2 *Let $A[z; \sigma]$ and \mathcal{M} be as above. Then the map*

$$\xi : A[z; \sigma] \longrightarrow \mathcal{M}$$

$$\sum_{l=0}^N z^{nl} \sum_{i=0}^{n-1} z^i [c_{i1}^l, c_{i2}^l, \dots, c_{in}^l] \longmapsto \sum_{l=0}^N t^l \begin{pmatrix} c_{01}^l & c_{12}^l & \cdots & \cdots & c_{n-1,n}^l \\ tc_{n-1,1}^l & c_{02}^l & \cdots & \cdots & c_{n-2,n}^l \\ \vdots & \ddots & \ddots & & \vdots \\ tc_{21}^l & & \ddots & \ddots & c_{1n}^l \\ tc_{11}^l & tc_{22}^l & \cdots & tc_{n-1,n-1}^l & c_{0n}^l \end{pmatrix} \quad (3.5)$$

is a ring isomorphism.

The identification of $A[z; \sigma]$ and \mathcal{M} was first shown in [11], where it has been studied for the more general situation of skew polynomial rings over arbitrary semisimple rings with a monomorphism σ . This general situation has also been used in [2] in order to classify certain group convolutional codes. Our choice of the semisimple ring A and the automorphism σ leads to a particularly simple proof which we would like to briefly present.

PROOF: It is obvious that each polynomial in $A[z; \sigma]$ has a unique representation as on the left hand side of (3.5). Thus the map ξ is well-defined. Moreover, it is obvious that ξ is bijective and additive, and it remains to show that it is multiplicative. In order to do so, we firstly observe that $\xi(\alpha) = \text{diag}(\alpha_1, \dots, \alpha_n)$ for any $\alpha = [\alpha_1, \dots, \alpha_n] \in A$, and secondly, that

$$\xi(z^{nl+i}) = t^l \begin{pmatrix} 0 & I_{n-i} \\ tI_i & 0 \end{pmatrix} = \begin{pmatrix} 0 & I_{n-1} \\ t & 0 \end{pmatrix}^{nl+i} \quad \text{for all } l \in \mathbb{N}_0 \text{ and } i = 0, \dots, n-1.$$

Now the identities $\xi(\alpha\beta) = \xi(\alpha)\xi(\beta)$, $\xi(z^{\nu+\mu}) = \xi(z^{\nu})\xi(z^{\mu})$, and $\xi(z^{\nu}\alpha) = \xi(z^{\nu})\xi(\alpha)$, where $\nu, \mu \in \mathbb{N}_0$ and $\alpha, \beta \in A$, are obvious, and one easily verifies $\xi(\alpha)\xi(z) = \xi(z)\xi(\sigma(\alpha))$ for all $\alpha \in A$. Using the additivity of ξ we conclude that ξ is indeed multiplicative, hence a ring isomorphism. \square

For later purposes it will be handy to have an explicit formula for the entries of $\xi(g)$. For

$$g := \sum_{l=0}^N z^{nl} \sum_{i=0}^{n-1} z^i [c_{i1}^l, c_{i2}^l, \dots, c_{in}^l] \quad (3.6)$$

and $\xi(g) = (m_{ab})$ one computes

$$m_{ab} = \sum_{l=0}^N t^{l+\text{sgn}(a-b)} c_{b-a+\text{sgn}(a-b)n,b}^l \quad \text{for } 1 \leq a, b \leq n, \quad (3.7)$$

where

$$\text{sgn}(x) := \begin{cases} 1 & \text{if } x > 0, \\ 0 & \text{else.} \end{cases}$$

It is clear that the subring $\xi(\mathbb{F}[z])$ of \mathcal{M} is given by the set of matrices

$$\sum_{l=0}^N t^l \begin{pmatrix} c_0^l & c_1^l & \cdots & \cdots & c_{n-1}^l \\ tc_{n-1}^l & c_0^l & \cdots & \cdots & c_{n-2}^l \\ \vdots & \ddots & \ddots & & \vdots \\ tc_2^l & & \ddots & \ddots & c_1^l \\ tc_1^l & tc_2^l & \cdots & tc_{n-1}^l & c_0^l \end{pmatrix} \quad \text{where } N \in \mathbb{N}_0, c_i^l \in \mathbb{F}, \quad (3.8)$$

and, defining $f \cdot M := \xi(f)M$ for $f \in \mathbb{F}[z]$ and $M \in \mathcal{M}$, we may impose a left $\mathbb{F}[z]$ -module structure on \mathcal{M} making it isomorphic to $A[z; \sigma]$ as left $\mathbb{F}[z]$ -modules. Due to the form of $\xi(f)$ as given in (3.8) the thus obtained module structure is of course not identical to the canonical $\mathbb{F}[t]$ -module structure of \mathcal{M} .

In the sequel we will translate various properties of polynomials in $A[z; \sigma]$ into matrix properties in \mathcal{M} . First of all we will show how to identify the units in \mathcal{M} . This will play an important role later on when discussing left ideals that are direct summands.

Proposition 3.3 *Let \mathcal{M}^\times be the group of units of \mathcal{M} . Then $\mathcal{M}^\times = \mathcal{M} \cap GL_n(\mathbb{F}[t])$. In other words, $M \in \mathcal{M}$ is a unit in the ring \mathcal{M} if and only if $\det(M) \in \mathbb{F}^\times := \mathbb{F} \setminus \{0\}$.*

As a consequence, left- (or right-) invertible elements in \mathcal{M} or in $A[z; \sigma]$ are units.

PROOF: The inclusion “ \subseteq ” is clear. For the inclusion “ \supseteq ” let $M \in \mathcal{M} \cap GL_n(\mathbb{F}[t])$. Then there exists a matrix $N \in GL_n(\mathbb{F}[t])$ such that $MN = I$. Substituting $t = 0$ we obtain $M(0)N(0) = I$, thus $N(0) = M(0)^{-1}$. Since $M \in \mathcal{M}$ the matrix $M(0)$ is upper triangular. But then the same is true for $N(0)$, showing that $N \in \mathcal{M}$. \square

Let us now turn to properties of the skew polynomial ring $A[z; \sigma]$ that follow from the semi-simplicity of A . Since the idempotents e_1, \dots, e_n are pairwise orthogonal and satisfy $e_1 + \dots + e_n = 1$ we have

$$A[z; \sigma] = \langle e_1 \rangle^\bullet \oplus \cdots \oplus \langle e_n \rangle^\bullet = \langle e_1 \rangle \oplus \cdots \oplus \langle e_n \rangle.$$

As a consequence, each element $g \in A[z; \sigma]$ has a unique decomposition

$$g = g^{(1)} + \dots + g^{(n)}, \quad \text{where } g^{(a)} := e_a g. \quad (3.9)$$

The following notions will play a central role. Recall that coefficients of skew polynomials are always meant to be right hand side coefficients.

Definition 3.4 Let $g \in A[z; \sigma]$.

- (a) For $a = 1, \dots, n$ we call $g^{(a)} := e_a g$ the a -th component of g .
- (b) The *support* of g is defined as $T_g := \{a \mid g^{(a)} \neq 0\}$.
- (c) We call g *delay-free* if $T_g = T_{g_0}$ where $g_0 \in A$ is the constant term of the polynomial g .
- (d) The polynomial g is said to be *semi-reduced* if the leading coefficients of the components $g^{(a)}$, $a \in T_g$, lie in pairwise different ideals $\langle e_{i_a} \rangle$.
- (e) The polynomial g is called *reduced* if no leading term of any component of g is a right divisor of a term of any other component of g .

In order to comment on these notions let us have a closer look at the components of a polynomial. Using (3.4) one obtains that, for instance, the first component of a polynomial g is of the form

$$g^{(1)} = [c_0, 0, \dots, 0] + z[0, c_1, 0, \dots, 0] + z^2[0, 0, c_2, 0, \dots, 0] + \dots = c_0 e_1 + z c_1 e_2 + z^2 c_2 e_3 + \dots$$

for some $c_j \in \mathbb{F}$. In general we derive from (3.4)

$$g^{(a)} = \sum_{j=0}^{N_a} z^j c_{a,j} e_{(a+j-1 \bmod n)+1} \text{ for some } N_a \in \mathbb{N}_0 \text{ and } c_{a,j} \in \mathbb{F} \quad (3.10)$$

for $a = 1, \dots, n$. In particular, the coefficients of the components are \mathbb{F} -multiples of primitive idempotents. As a consequence, g is semi-reduced if and only if no leading term of any component of g is a right divisor of the leading term of any other component of g . Obviously, reducedness implies semi-reducedness, and a polynomial consisting of one component is always reduced.

The concept of reducedness has been introduced for the skew polynomial ring $A[z; \sigma]$ in [8, Def. 4.9]. It proved to be very useful in the theory of CCC's. In particular, it has led to the following results concerning minimal encoder matrices and Forney indices of CCC's, see [8, Thm. 4.5, Thm. 4.15, Prop. 7.10, Thm. 7.13(b)].

Theorem 3.5 *As before let $n \mid (q-1)$. Let σ be any automorphism in $\text{Aut}_{\mathbb{F}}(A)$ and consider the identification \mathfrak{p} of $\mathbb{F}[z]^n$ with the skew polynomial ring $A[z; \sigma]$ as given in (2.4) and where we identify A with the quotient ring $\mathbb{F}[x]/\langle x^n - 1 \rangle$.*

- (1) *For every $g \in A[z; \sigma]$ there exists a unit $u \in A[z; \sigma]^\times$ such that ug is reduced.*
- (2) *Let $\mathcal{C} \subseteq \mathbb{F}[z]^n$ be a σ -CCC. Then there exists a reduced and delay-free polynomial $g \in A[z; \sigma]$ such that $\mathfrak{p}(\mathcal{C}) = \langle g \rangle := \{fg \mid f \in A[z; \sigma]\}$. In particular, the left ideal $\mathfrak{p}(\mathcal{C})$ is principal. Moreover, the polynomial g is unique up to left multiplication by units in A .*
- (3) *Let $g \in A[z; \sigma]$ be a reduced polynomial. Then $\mathfrak{p}^{-1}(\langle g \rangle) \subseteq \mathbb{F}[z]^n$ is a direct summand of $\mathbb{F}[z]^n$ if and only if $g = \sum_{l \in T_g} u^{(l)}$ for some unit $u \in A[z; \sigma]$. That is, the σ -CCC's are obtained by taking any unit u in $A[z; \sigma]$ and choosing any collection of components of u that forms a reduced polynomial.*
- (4) *Let $g \in A[z; \sigma]$ be a reduced polynomial with support $T_g = \{i_1, \dots, i_k\}$. Then $\mathcal{C} := \mathfrak{p}^{-1}(\langle g \rangle) = \text{im } G = \{uG \mid u \in \mathbb{F}[z]^k\}$, where*

$$G := \begin{pmatrix} \mathfrak{p}^{-1}(g^{(i_1)}) \\ \vdots \\ \mathfrak{p}^{-1}(g^{(i_k)}) \end{pmatrix} \in \mathbb{F}[z]^{k \times n}. \quad (3.11)$$

Furthermore, if \mathcal{C} is a direct summand of $\mathbb{F}[z]^n$ then G is a minimal encoder matrix of \mathcal{C} . As a consequence, \mathcal{C} is a σ -CCC of dimension k with Forney indices $\deg g^{(i_1)}, \dots, \deg g^{(i_k)}$ and degree $\delta := \sum_{l=1}^k \deg g^{(i_l)}$.

Let us now return to the situation where σ is as in (3.3). Throughout this paper semi-reduced polynomials will be much more handy than reduced ones, see Proposition 3.10(4)

below. Fortunately, it can easily be confirmed that the weaker notion of semi-reducedness is sufficient for the results above to be true. We confine ourselves to presenting the following details.

Remark 3.6 The results of Theorem 3.5(1) – (4), except for the uniqueness result in (2), are true for semi-reduced polynomials as well. In order to see this, one has to confirm that, firstly, all results of [8, Section 4], in particular Proposition 4.10, Corollary 4.13, and Lemma 4.14, with the exception of the uniqueness result in Theorem 4.15, remain true for semi-reduced polynomials. Secondly one can easily see that Theorem 7.8, Proposition 7.10, Corollary 7.11, Theorem 7.13, and Corollary 7.15 of [8, Section 7] remain true if one replaces reducedness by semi-reducedness. In all cases the proofs in [8] remain literally the same.

Due to part (3) of the theorem above the following notion will be important to us.

Definition 3.7 A polynomial $g \in A[z; \sigma]$ is called *basic* if there exists a unit $u \in A[z; \sigma]^\times$ such that $g = \sum_{l \in T_g} u^{(l)}$.

According to part (3) and (4) of Theorem 3.5, see also Remark 3.6, a semi-reduced polynomial g is basic if and only if the matrix G in (3.11) is basic.

Let us now have a closer look at semi-reduced polynomials. From (3.10) we see immediately that

$$g \text{ is semi-reduced} \iff \begin{cases} \text{the numbers } (a + \deg g^{(a)} - 1 \bmod n) + 1, & a \in T_g, \\ \text{are pairwise different.} \end{cases} \quad (3.12)$$

Moreover, one has

$$g \in A[z; \sigma]^\times \text{ and } g \text{ semi-reduced} \implies g \in A^\times. \quad (3.13)$$

Indeed, suppose $1 = hg = (he_1 + \dots + he_n)g = \sum_{l=1}^n he_l g$. Since $\langle e_l \rangle \cong \mathbb{F}$ we get $\deg(he_l g) = \deg(he_l) + \deg(e_l g)$ and the leading coefficient of $he_l g$ is in the same ideal as the leading coefficient of $g^{(l)}$. Now semi-reducedness of g shows that no cancelation of the leading coefficients in $\sum_{l=1}^n he_l g$ is possible and thus $hg = 1$ implies that $\deg(g^{(l)}) = 0$ for all $l = 1, \dots, n$.

It is easy to translate these notions into the setting of the matrix ring \mathcal{M} . Indeed, defining the standard basis matrices

$$E_{ab} \in \mathbb{F}^{n \times n} \text{ via } (E_{ab})_{ij} = \begin{cases} 1 & \text{if } (i, j) = (a, b) \\ 0 & \text{if } (i, j) \neq (a, b) \end{cases} \text{ for } a, b = 1, \dots, n \quad (3.14)$$

we obtain

$$\xi(e_a) = E_{aa}. \quad (3.15)$$

Thus,

$$\xi(g^{(a)}) = \xi(e_a)\xi(g) = E_{aa}\xi(g) \quad (3.16)$$

is a matrix where at most the a -th row is nonzero. It is obtained from $\xi(g)$ by deleting all other rows. This gives rise to the following definition.

Definition 3.8 Let $M = (m_{ab}) \in \mathcal{M}$. Then we define the support of M to be

$$\text{Supp}(M) := \{a \mid \text{the } a\text{-th row of } M \text{ is non-zero}\}.$$

We say that M is *delay-free* if $m_{aa}(0) \neq 0$ for all $a \in \text{Supp}(M)$.

By definition $\text{Supp}(\xi(g)) = T_g$ for all $g \in A[z; \sigma]$. Furthermore, the very definition of ξ shows that g is delay-free if and only if $\xi(g)$ is. Finally, we have the implication

$$g \text{ is delay-free} \implies \text{rank}_{\mathbb{F}[t]} \xi(g) = \text{rank}_{\mathbb{F}} \xi(g)|_{t=0} = |T_g|. \quad (3.17)$$

This follows by observing that the nonzero rows of $\xi(g)|_{t=0}$ form a matrix in row echelon form with pivot positions in the columns with indices in T_g .

In order to express semi-reducedness in terms of the matrix $\xi(g)$ we need the following concept.

Definition 3.9 Let $M = (m_{ab}) \in \mathcal{M}$ and put $d_{ab} := \deg(m_{ab})$ for $a, b = 1, \dots, n$ (where, as usual, the zero polynomial has degree $-\infty$). The *degree matrix* of M is defined as

$$\mathcal{D}(M) = \begin{pmatrix} nd_{11} & nd_{12} + 1 & nd_{13} + 2 & \cdots & nd_{1n} + n - 1 \\ nd_{21} - 1 & nd_{22} & nd_{23} + 1 & \cdots & nd_{2n} + n - 2 \\ nd_{31} - 2 & nd_{32} - 1 & nd_{33} & \cdots & nd_{3n} + n - 3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ nd_{n1} - n + 1 & nd_{n2} - n + 2 & nd_{n3} - n + 3 & \cdots & nd_{nn} \end{pmatrix}.$$

Hence $\mathcal{D}(M)_{ab} = nd_{ab} - a + b \in \mathbb{N}_0 \cup \{-\infty\}$ for $a, b = 1, \dots, n$. We call a row of $\mathcal{D}(M)$ *trivial* if all entries are $-\infty$. The matrix M is said to be *semi-reduced* if the maxima in the non-trivial rows of $\mathcal{D}(M)$ appear in different columns.

Obviously, the trivial rows of $\mathcal{D}(M)$ correspond to the zero rows of M . Furthermore, we have the following properties.

Proposition 3.10 Let $g \in A[z; \sigma]$ and $M = \xi(g) = (m_{ab})$. For $a, b = 1, \dots, n$ put $d_{ab} = \deg m_{ab}$.

- (1) In each row and column of $\mathcal{D}(M)$ the entries different from $-\infty$ are pairwise different. In particular, each non-trivial row has a unique maximum.
- (2) For all $a, b = 1, \dots, n$ we have $\xi(g^{(a)}e_b) = E_{aa}ME_{bb} = m_{ab}E_{ab}$ and $\deg(g^{(a)}e_b) = \mathcal{D}(M)_{ab}$. Furthermore,

$$\deg g^{(a)} = \max_{1 \leq b \leq n} \mathcal{D}(M)_{ab} \text{ for all } a = 1, \dots, n \quad (3.18)$$

and

$$\deg g = \max_{1 \leq a \leq n} (\deg g^{(a)}) = \max_{1 \leq a, b \leq n} \mathcal{D}(M)_{ab}.$$

- (3) g is semi-reduced if and only if M is semi-reduced.

- (4) For $a \in \text{Supp}(M)$ let $\delta_a := \max\{d_{ab} \mid 1 \leq b \leq n\}$ and put $b_a := \max\{b \mid d_{ab} = \delta_a\}$; that is, m_{a,b_a} is the rightmost entry in the a -th row of M having maximal degree δ_a . Then $\max_{1 \leq b \leq n} \mathcal{D}(M)_{ab} = \mathcal{D}(M)_{a,b_a}$. As a consequence, M is semi-reduced if and only if the indices $b_a, a \in \text{Supp}(M)$, are pairwise different.

PROOF: Part (1) is trivial. The first assertion of (2) follows from (3.15) and the multiplicativity of ξ . As for the degree of $g^{(a)}e_b$ let g be as in (3.6). Using (3.4) we obtain

$$e_a g = \sum_{l \geq 0} \sum_{i=0}^{n-1} z^{nl+i} c_{i,(i+a-1 \bmod n)+1}^l e_{(i+a-1 \bmod n)+1}.$$

Notice that for any $b = 1, \dots, n$ we have

$$e_{(i+a-1 \bmod n)+1} e_b = e_b \iff (i+a-1 \bmod n) + 1 = b \iff i = b - a + \text{sgn}(a-b)n$$

while $e_{(i+a-1 \bmod n)+1} e_b = 0$ for all other values of $i \in \{0, \dots, n-1\}$. Thus

$$g^{(a)}e_b = e_a g e_b = \sum_{l \geq 0} z^{n(l+\text{sgn}(a-b))+b-a} c_{b-a+\text{sgn}(a-b)n,b}^l e_b.$$

As a consequence,

$$\deg(g^{(a)}e_b) = \left(\max\{l \mid c_{b-a+\text{sgn}(a-b)n,b}^l \neq 0\} + \text{sgn}(a-b) \right) n + b - a = n \deg(m_{ab}) + b - a,$$

where the last identity follows from (3.7). This shows $\deg(g^{(a)}e_b) = \mathcal{D}(M)_{ab}$. The last two statements of (2) are a direct consequence. For parts (3) and (4) let δ_a and b_a be as in (4). Then $\max\{\mathcal{D}(M)_{ab} \mid 1 \leq b \leq n\} = \max\{nd_{ab} - a + b \mid 1 \leq b \leq n\} = n\delta_a - a + b_a = \mathcal{D}(M)_{a,b_a}$. Now the rest of (4) is a consequence of Definition 3.9, whereas (3) follows from (3.12) along with part (2) since $a + \deg g^{(a)} - 1 \bmod n = b_a - 1$. \square

Let us consider some examples.

Example 3.11 Let α be a primitive element of \mathbb{F} and put $n = q - 1$. Then $x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i)$. Consider the isomorphism $\phi : A' \longrightarrow A$, $f \mapsto [f(1), f(\alpha), \dots, f(\alpha^{n-1})]$ of $A' := \mathbb{F}[x]/\langle x^n - 1 \rangle$ with A . Then the primitive idempotents of A' are given by $e_a := \gamma_a \prod_{i \neq a-1} (x - \alpha^i)$ for $a = 1, \dots, n$ and some constants $\gamma_a \in \mathbb{F}^\times$. Choose now the automorphism $\sigma \in \text{Aut}_{\mathbb{F}}(A')$ defined via $\sigma(x) = \alpha^{-1}x$. Then one easily checks that (3.4) is satisfied. This example has also been studied in [5, Prop. 4.2] (since in that paper the automorphism is given by $x \mapsto \alpha x$ one has to replace α by α^{-1} in the idempotents in order to get back the ordering as in [5]). In [5, Prop. 4.2, Thm. 2.1] it has been shown that for any $1 \leq \delta \leq n-1$ the σ -cyclic submodule $\mathcal{C} = \mathfrak{p}^{-1}(\langle g \rangle)$, where $g = e_1 \sum_{i=0}^{\delta} z^i$, gives rise to a 1-dimensional MDS convolutional code. Hence the distance of that code is $n(\delta+1)$, which is the maximum value among all 1-dimensional codes of length n and degree δ (for MDS convolutional codes see [22]). Let us compute an encoder matrix $G \in \mathbb{F}[z]^{1 \times n}$ of \mathcal{C} . From Theorem 3.5(4) we know that $G = \mathfrak{p}^{-1}(g)$ is such an encoder since $g = g^{(1)}$. The

first primitive idempotent in A' is given by $e_1 = \frac{1}{n} \sum_{i=0}^{n-1} x^i$ as one can easily verify via the isomorphism ϕ . Thus,

$$g = \frac{1}{n} \sum_{i=0}^{n-1} x^i \sum_{j=0}^{\delta} z^j = \frac{1}{n} \sum_{j=0}^{\delta} z^j \sum_{i=0}^{n-1} \sigma^j(x^i) = \frac{1}{n} \sum_{j=0}^{\delta} z^j \sum_{i=0}^{n-1} \alpha^{-ji} x^i.$$

Using the map \mathbf{p} from (2.4) we obtain

$$G = \frac{1}{n} \left(\sum_{j=0}^{\delta} z^j, \sum_{j=0}^{\delta} z^j \alpha^{-j}, \dots, \sum_{j=0}^{\delta} z^j \alpha^{-(n-1)j} \right) = \frac{1}{n} \sum_{j=0}^{\delta} z^j (1, \alpha^{-j}, \alpha^{-2j}, \dots, \alpha^{-(n-1)j}).$$

In this specific example the matrix $M := \xi(g)$ has a particularly simple form. Indeed, since $g = g^{(1)} = \sum_{i=0}^{\delta} z^i e_{1+i}$ and $\delta \leq n-1$ we obtain

$$M := \xi(g) = \begin{pmatrix} \overbrace{1 \ 1 \ \dots \ 1}^{\delta+1} & 0 & \dots & 0 \\ & 0 & & \end{pmatrix} \text{ and } \mathcal{D}(M) = \begin{pmatrix} 0 & 1 & \dots & \delta & -\infty & \dots & -\infty \\ & -\infty & & \end{pmatrix}.$$

The degree equation (3.18) is obvious. Notice that the matrix M is idempotent. Thus, g is an idempotent generator of the left ideal $\bullet\langle g \rangle$.

Example 3.12 Let $q = 5$ and $n = 4$. Consider the matrix

$$M = \begin{pmatrix} 2+t & 1 & 4 & 4 \\ 0 & 1 & 3 & 0 \\ 4t & 2t & 1+t & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in \mathcal{M}.$$

Obviously, M is delay-free. The corresponding polynomial $g = \xi^{-1}(M) \in A[z; \sigma]$ is given by

$$g = 2e_1 + e_2 + e_3 + z(e_2 + 3e_3 + e_4) + z^2(4e_1 + 4e_3) + z^3(2e_2 + 4e_4) + z^4(e_1 + e_3),$$

and its components are

$$g^{(1)} = 2e_1 + ze_2 + 4z^2e_3 + 4z^3e_4 + z^4e_1, \quad g^{(2)} = e_2 + 3ze_3, \quad g^{(3)} = e_3 + ze_4 + 4z^2e_1 + 2z^3e_2 + z^4e_3.$$

The matrix, and thus g , are not semi-reduced as we can see directly from Proposition 3.10(4) or from the degree matrix

$$\mathcal{D}(M) = \begin{pmatrix} 4 & 1 & 2 & 3 \\ -\infty & 0 & 1 & -\infty \\ 2 & 3 & 4 & 1 \\ -\infty & -\infty & -\infty & -\infty \end{pmatrix}.$$

Using two steps of elementary row operations one can bring M into semi-reduced form without changing the left ideal $\bullet\langle M \rangle$. Indeed, one easily checks that

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 3t & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2+t & 1 & 4 & 4 \\ 0 & 1 & 3 & 0 \\ 4t & 2t & 1+t & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 4t & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} =: \bar{M}. \quad (3.19)$$

Since the two leftmost matrices are in \mathcal{M}^\times , see Proposition 3.3, we have $\bullet\langle M \rangle = \bullet\langle \bar{M} \rangle$. Furthermore, \bar{M} is semi-reduced as one can easily see with the help of Proposition 3.10(4). The corresponding polynomial $\bar{g} := \xi^{-1}(\bar{M})$ is given by $\bar{g} = 2e_1 + e_2 + e_3 + z(e_2 + 3e_3 + e_4) + z^2 4e_1$, which is semi-reduced according to Proposition 3.10(3). We will come back to this example later on in Example 4.4.

The procedure of semi-reducing matrices in \mathcal{M} as in the previous example always works. This is shown in the following result.

Theorem 3.13 *A matrix in $GL_n(\mathbb{F}[t])$ is said to be an elementary unit of \mathcal{M} if it is of any of the following types:*

- (i) $\sum_{i \neq a} E_{ii} + \alpha E_{aa}$ for some $\alpha \in \mathbb{F}^\times$ and $a = 1, \dots, n$,
- (ii) $I_n + t^N \alpha E_{ab}$ for some $N \geq 0$, $\alpha \in \mathbb{F}$ and $1 \leq a < b \leq n$,
- (iii) $I_n + t^N \alpha E_{ab}$ for some $N > 0$, $\alpha \in \mathbb{F}$ and $1 \leq b < a \leq n$.

Then each matrix in \mathcal{M} can be brought into semi-reduced form via left multiplication by finitely many elementary units of \mathcal{M} . As a consequence, each unit $M \in \mathcal{M}^\times$ can be written as a product of elementary units of \mathcal{M} .

PROOF: It is trivial that each of the matrices in (i) – (iii) is indeed in \mathcal{M}^\times , and that the inverse of such an elementary unit is an elementary unit of the same type.

Let now $M = (m_{ab}) \in \mathcal{M}$ and assume that M is not semi-reduced. Then, according to Proposition 3.10 there exist indices (a, c) and (b, c) where $b > a$ such that $\mathcal{D}(M)_{a,c}$ and $\mathcal{D}(M)_{b,c}$ are the maxima in the a -th and b -th row of $\mathcal{D}(M)$, respectively. Using the definition of the matrix $\mathcal{D}(M)$ one easily checks that for $b > a$ and $j = 1, \dots, n$

$$\mathcal{D}(M)_{bj} < \mathcal{D}(M)_{aj} \iff \deg(m_{bj}) \leq \deg(m_{aj}). \quad (3.20)$$

We want to transform M into semi-reduced form via left multiplication by elementary units of \mathcal{M} . Consider first the case $\mathcal{D}(M)_{bc} \leq \mathcal{D}(M)_{ac}$. Put $\hat{M} = (\hat{m}_{ij}) = (I_n + t^N \alpha E_{ab})M$ where $N := \deg(m_{ac}) - \deg(m_{bc}) \geq 0$ and $\alpha \in \mathbb{F}$ is such that $\deg(\hat{m}_{ac}) = \deg(m_{ac} + t^N \alpha m_{bc}) < \deg(m_{ac})$. This is possible due to (3.20). Then $\mathcal{D}(\hat{M})_{ac} < \mathcal{D}(M)_{ac}$. Furthermore, for $j \neq c$ we have $\hat{m}_{aj} = m_{aj} + t^N \alpha m_{bj}$ and thus

$$\begin{aligned} \mathcal{D}(\hat{M})_{aj} &= n \deg(\hat{m}_{aj}) - a + j \leq n \max\{\deg(m_{aj}), N + \deg(m_{bj})\} - a + j \\ &= \max\{n \deg(m_{aj}) - a + j, nN + n \deg(m_{bj}) - a + j\} \\ &= \max\{\mathcal{D}(M)_{aj}, \mathcal{D}(M)_{bj} + nN + b - a\} \\ &< \max\{\mathcal{D}(M)_{ac}, \mathcal{D}(M)_{bc} + nN + b - a\}, \end{aligned}$$

where the last inequality holds true due to the uniqueness of the row maxima in $\mathcal{D}(M)$ (see Proposition 3.10(1)). Since

$$\mathcal{D}(M)_{bc} + nN + b - a = n \deg(m_{bc}) - b + c + nN + b - a = n \deg(m_{ac}) - a + c = \mathcal{D}(M)_{ac}$$

the above results in $\mathcal{D}(\hat{M})_{aj} < \mathcal{D}(M)_{ac}$ for all $j = 1, \dots, n$.

If $\mathcal{D}(M)_{bc} > \mathcal{D}(M)_{ac}$, then put $\hat{M} := (I_n + t^N \alpha E_{ba})M$ where $N > 0$ and $\alpha \in \mathbb{F}$ are chosen such that $\deg(m_{bc} + t^N \alpha m_{ac}) < \deg(m_{bc})$. Again, this is possible by virtue of (3.20). Arguing the same way we obtain likewise $\mathcal{D}(\hat{M})_{bj} < \mathcal{D}(M)_{bc}$ for all $j = 1, \dots, n$. Summarizing we see that if M is not semi-reduced we may apply one of the two transformations given above, and they both strictly decrease the maximum value in one of the rows of $\mathcal{D}(M)$ while all other rows remain unchanged. Altogether this results in a reduction procedure that must stop after finitely many steps with a semi-reduced matrix.

The last statement of the theorem follows directly from (3.13) together with the use of elementary units of Type (i). \square

One easily checks that the elementary units in Theorem 3.13 correspond to the units

$$\xi^{-1}\left(\sum_{i \neq a} E_{ii} + \alpha E_{aa}\right) = \alpha e_a + \sum_{i \neq a} e_i, \quad \xi^{-1}(I_n + t^N \alpha E_{ab}) = 1 + z^{Nn+b-a} \alpha e_b,$$

in $A[z; \sigma]$. Of course, in the second case we have $a \neq b$ and $N > 0$ if $b < a$. These units in $A[z; \sigma]$ have been studied in detail in the paper [6]. In a more general context it has been shown in [6, Lem. 3.7] that $1 + z^d \alpha e_b$, where $d > 0$, is a unit if and only if $n \nmid d$, and that each unit in $A[z; \sigma]$ can be written as the product of finitely many units of the types above. This corresponds exactly to our last statement in Theorem 3.13 above. With that theorem we even see that left reduction to a semi-reduced polynomial in the skew-polynomial ring $A[z; \sigma]$, cf. [8, Cor. 4.13], simply means elementary row reduction of the matrices in \mathcal{M} .

The following result tells us as to when a matrix in \mathcal{M} can be completed to a unit in \mathcal{M} by filling in suitable entries in the zero rows. This result will be important later on when studying whether a cyclic submodule is a direct summand.

Lemma 3.14 *Let $M \in \mathcal{M}$ be delay-free and $\text{Supp}(M) = \{i_1, \dots, i_k\}$, where $i_1 < \dots < i_k$. Denote the rows of M by M_1, \dots, M_n . Then the following are equivalent.*

(a) *The matrix $\widetilde{M} := \begin{pmatrix} M_{i_1} \\ \vdots \\ M_{i_k} \end{pmatrix}$ is basic.*

(b) *There exist vectors $\widehat{M}_i \in \mathbb{F}[t]^{1 \times n}$ for $i \in \{1, \dots, n\} \setminus \{i_1, \dots, i_k\}$ such that the matrix*

$$N = \begin{pmatrix} N_1 \\ \vdots \\ N_n \end{pmatrix} \in \mathbb{F}[t]^{n \times n}, \text{ where } N_i := \begin{cases} M_i & \text{if } i \in \{i_1, \dots, i_k\} \\ \widehat{M}_i & \text{if } i \in \{1, \dots, n\} \setminus \{i_1, \dots, i_k\} \end{cases}$$

is in \mathcal{M}^\times .

Since every matrix in \mathcal{M}^\times is delay-free it is clear that the delay-freeness is necessary for the implication (a) \implies (b) to be true.

For the proof the following suggestive notation will be helpful. Arbitrary entries of a matrix in $\mathbb{F}[t]^{r \times n}$ will be indicated by an asterisk $*$, whereas entries that are multiples of t will be denoted by the symbol $\langle t \rangle$. Thus, the elements of \mathcal{M} are just the matrices of the form

$$\begin{pmatrix} * & * & \cdots & * \\ \langle t \rangle & * & & * \\ \vdots & \ddots & \ddots & \vdots \\ \langle t \rangle & \cdots & \langle t \rangle & * \end{pmatrix}.$$

PROOF: Only the implication “(a) \Rightarrow (b)” requires proof. It is a well-known fact that, since the k -minors of \widetilde{M} are coprime, there exists a matrix $\widehat{M} \in \mathbb{F}[t]^{(n-k) \times n}$ such that $N := \begin{pmatrix} \widetilde{M} \\ \widehat{M} \end{pmatrix} \in GL_n(\mathbb{F}[t])$. Therefore, N is of the form

$$\begin{pmatrix} \langle t \rangle & \cdots & m_{i_1 i_1} & * & \cdots & & * \\ \langle t \rangle & \cdots & \cdots & \cdots & m_{i_2 i_2} & * & \cdots & * \\ \vdots & & & & & & & \vdots \\ \langle t \rangle & \cdots & \cdots & \cdots & \cdots & \cdots & m_{i_k i_k} & * \cdots * \end{pmatrix},$$

\widehat{M}

where all entries in the upper block and to the left of m_{i_j, i_j} are of the type $\langle t \rangle$. We will show now that with suitable row operations we can transform N into a matrix being in \mathcal{M} without altering the rows of the upper part \widetilde{M} . By delay-freeness of M we have $m_{i_j i_j}(0) \neq 0$ for all $j = 1, \dots, k$. Hence, by adding suitable multiples of rows of \widetilde{M} to \widehat{M} we can transform N into a matrix of the form

$$\begin{pmatrix} \langle t \rangle & \cdots & m_{i_1 i_1} & * & \cdots & & * \\ \langle t \rangle & \cdots & \cdots & \cdots & m_{i_2 i_2} & * & \cdots & * \\ \vdots & & & & & & & \vdots \\ \langle t \rangle & \cdots & \cdots & \cdots & \cdots & \cdots & m_{i_k i_k} & * \cdots * \\ \hline & \langle t \rangle & & \langle t \rangle & & \langle t \rangle & & \\ * & \vdots & * & \vdots & * & \vdots & * & \end{pmatrix} \in GL_n(\mathbb{F}[t]), \quad (3.21)$$

where the upper part \widetilde{M} is unaltered. Therefore, we may assume without loss of generality that N is as in (3.21). For the next step observe that for any column vector $a \in \mathbb{F}[t]^{l \times 1}$ there exists $U \in GL_l(\mathbb{F}[t])$ such that Ua is of the form

$$\begin{pmatrix} * \\ \langle t \rangle \\ \vdots \\ \langle t \rangle \end{pmatrix}.$$

Thus, working consecutively from the left to the right and applying suitable elementary row operations on the lower block of N we can bring \widehat{M} into the form

$$\widehat{M} = \left(\begin{array}{ccc|ccc|ccc} * & & & \langle t \rangle & & & & & & \\ \langle t \rangle & \ddots & & \vdots & & & & & & \\ & & \ddots & * & \langle t \rangle & & & & & \\ \hline \langle t \rangle & \cdots & \langle t \rangle & \langle t \rangle & * & & \langle t \rangle & & & \\ \vdots & & \vdots & \vdots & \langle t \rangle & \ddots & \vdots & & & \\ \vdots & & \vdots & \vdots & & \ddots & * & \langle t \rangle & & \\ \hline \vdots & & \vdots & \vdots & \vdots & \langle t \rangle & \langle t \rangle & \ddots & & \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & & \ddots & \\ \langle t \rangle & \cdots & \langle t \rangle & \langle t \rangle & \langle t \rangle & \langle t \rangle & \langle t \rangle & & & \end{array} \right) \left. \begin{array}{l} \left. \begin{array}{l} \vdots \\ \vdots \\ \vdots \end{array} \right\} i_1 - 1 \text{ rows} \\ \left. \begin{array}{l} \vdots \\ \vdots \\ \vdots \end{array} \right\} i_2 - i_1 - 1 \text{ rows} \end{array} \right\}$$

$\underbrace{\hspace{10em}}_{i_1 \text{ columns}} \quad \underbrace{\hspace{10em}}_{i_2 - i_1 \text{ columns}}$

while \widetilde{M} does not change. Assume that $N = \begin{pmatrix} \widetilde{M} \\ \widetilde{M} \end{pmatrix}$ is of this form and recall that the j -th row of \widetilde{M} is given by M_{i_j} , $j = 1, \dots, k$. Now, moving for $j = 1, \dots, k$ the j -th row of \widetilde{M} to the bottom of the j -th block of \widehat{M} we can form a matrix N' where the i_j -th row is given by M_{i_j} for $j = 1, \dots, k$ and where we keep the ordering of all remaining rows of N . This way, the entries in \widehat{M} that are explicitly indicated by asterisks and the entries $m_{i_j i_j}$, $j = 1, \dots, k$, will appear on the diagonal of N' , while all entries below the diagonal will be in $\langle t \rangle$. Hence $N' \in GL_n(\mathbb{F}[t]) \cap \mathcal{M}$ and Proposition 3.3 completes the proof. \square

Remark 3.15 Essentially all of the results of this section are true without the requirement of n dividing $q - 1$. Indeed, just consider A and σ as in (3.1) and (3.3). Section 4 of [8] remains true in this case since it was solely based on A being a direct product of fields. The only part that needs extra proof is part (3) of Theorem 3.5, and that can be accomplished using ring theoretic methods. Part (4) of that theorem does not have a meaning in this more general setting since A is not isomorphic to $\mathbb{F}[x]/\langle x^n - 1 \rangle$ anymore, and thus the map \mathfrak{p} does not exist. We will briefly come back to this situation in Section 6.

4 Construction and Existence of σ -CCC's

In this section we will apply the results obtained so far in order to construct σ -CCC's, and we will discuss some existence issues. As before, let A and σ be as in (3.1) and (3.3) and let $n \mid (q - 1)$. Moreover, put

$$\mathcal{M}_{\text{basic}} := \left\{ M \in \mathcal{M} \left| \begin{array}{l} M \text{ delay-free and} \\ \text{the nonzero rows of } M \text{ form a basic matrix} \end{array} \right. \right\}. \quad (4.1)$$

Let us summarize the previous results in the following form. We also think it is worthwhile pointing out that the property of a module being a direct summand as an $\mathbb{F}[z]$ -submodule is equivalent to being a direct summand as a left ideal in the skew polynomial ring. Recall the map \mathfrak{p} from (2.4).

Theorem 4.1 *Let $g \in A[z; \sigma]$ be delay-free and semi-reduced. Then the following are equivalent.*

- (i) $\langle g \rangle$ is a direct summand of the left $\mathbb{F}[z]$ -module $A[z; \sigma]$ (thus, $\mathfrak{p}^{-1}(\langle g \rangle)$ is a σ -CCC).
- (ii) $\langle g \rangle$ is a direct summand of the ring $A[z; \sigma]$.
- (iii) $\xi(g) \in \mathcal{M}_{\text{basic}}$.

PROOF: The equivalence of (i) and (ii) has been proved in [6, Rem. 2.10], whereas (i) \iff (iii) follows from Lemma 3.14, Theorem 3.5(3), and the fact that ξ is an isomorphism. \square

Notice that (iii) gives us an easy way of checking whether a given left ideal is a direct summand (thus a σ -CCC) since basicness of a matrix in $\mathbb{F}[t]^{k \times n}$ can, for instance, be checked by testing whether its k -minors are coprime.

As a consequence, σ -CCC's are in one-one correspondence with the left ideals $\langle M \rangle \subseteq \mathcal{M}$ where $M \in \mathcal{M}_{\text{basic}}$ is semi-reduced. Proposition 3.10(3) and Theorem 3.5(4), see also Remark 3.6, tell us immediately the algebraic parameters of the code, that is, the dimension, the Forney indices and degree. This is summarized in the next result.

Corollary 4.2 *Let $M \in \mathcal{M}_{\text{basic}}$ be semi-reduced and let $\text{Supp}(M) = \{i_1, \dots, i_k\}$, where $i_1 < \dots < i_k$. Then $\mathcal{C} := \mathfrak{p}^{-1}(\langle \xi^{-1}(M) \rangle) \subseteq \mathbb{F}[z]^n$ is a k -dimensional σ -CCC with Forney indices given by $\nu_l := \max_{1 \leq j \leq n} \mathcal{D}(M)_{i_l, j}$ for $l = 1, \dots, k$.*

Example 4.3 Let us consider again the setting of Example 3.11 where $n = q - 1$ and $\sigma(x) = \alpha^{-1}x$ with some primitive element α of \mathbb{F} . In that example we presented some 1-dimensional σ -cyclic MDS convolutional codes. These codes can be generalized as follows. Let $g = (e_1 + e_2)(1 + z)$. Then

$$M = \xi(g) = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 \\ & & 0 & & & \end{pmatrix}, \quad \mathcal{D}(M) = \begin{pmatrix} 0 & 1 & -\infty & -\infty & \dots & -\infty \\ 0 & 0 & 1 & -\infty & \dots & -\infty \\ & & -\infty & & & \end{pmatrix}.$$

Obviously, $M \in \mathcal{M}_{\text{basic}}$ and hence the previous corollary guarantees that $\mathcal{C} := \mathfrak{p}^{-1}(\langle g \rangle) \subseteq \mathbb{F}[z]^n$ is a σ -CCC. Furthermore, M , and thus g , is semi-reduced. As a consequence, the code \mathcal{C} is a 2-dimensional code in $\mathbb{F}[z]^n$ with both Forney indices equal to 1 and degree 2. In other words, \mathcal{C} is a unit memory code. We will show now that these codes are optimal in the sense that they have the largest distance among all 2-dimensional codes with Forney indices 1, 1 and length $n = q - 1$ over \mathbb{F}_q . According to [9, Prop. 4.1] (see also [6, Eq. (1.3)]) the largest possible distance for codes with these parameters, called the Griesmer bound, is given by the number $2(n - 1)$. In order to compute the actual distance of \mathcal{C} we need an encoder matrix. Since the support of g is $T_g = \{1, 2\}$ and $g^{(1)} = e_1 + ze_2$, $g^{(2)} = e_2 + ze_3$, Theorem 3.5(4) tells us that a minimal encoder is given by the matrix $G = G_0 + G_1z$ where

$$G_0 = \begin{pmatrix} \mathfrak{p}^{-1}(e_1) \\ \mathfrak{p}^{-1}(e_2) \end{pmatrix}, \quad G_1 = \begin{pmatrix} \mathfrak{p}^{-1}(e_2) \\ \mathfrak{p}^{-1}(e_3) \end{pmatrix} \in \mathbb{F}^{2 \times n}.$$

Furthermore, G is basic and minimal, and thus $\text{rank } G_0 = \text{rank } G_1 = 2$. Now it is easy to see that the two block codes generated by G_0 and G_1 , respectively, are MDS codes,

that is, they both have distance $n - 1$. Indeed, recall from Example 3.11 that $e_a = \gamma_a \prod_{i \neq a-1} (x - \alpha^i)$ for $a = 1, \dots, n$. Thus, in the ring $A' = \mathbb{F}[x]/\langle x^n - 1 \rangle$ the ideal $\langle e_1, e_2 \rangle$ is identical to $\langle f \rangle$, where $f = \prod_{i=2}^{n-1} (x - \alpha^i)$. As a consequence, the cyclic block code $\text{im } G_0 = \mathfrak{p}^{-1}(\langle e_1, e_2 \rangle) = \mathfrak{p}^{-1}(\langle f \rangle) \subseteq \mathbb{F}^n$ has designed distance $n - 1$. The second block code $\langle e_2, e_3 \rangle$ is simply the image of the first one under the map σ . Since σ is weight-preserving this shows that the second code has distance $n - 1$, too. But now it is clear that the convolutional code \mathcal{C} has distance $2(n - 1)$ since for each message $u = \sum_{j=0}^N u_j z^j \in \mathbb{F}[z]^2$, where $u_0 \neq 0 \neq u_N$, the corresponding codeword uG has constant term $u_0 G_0$ and highest coefficient $u_N G_1$, both of weight at least $n - 1$.

In the same way one can proceed and consider the unit memory code generated by the polynomial $g = (e_1 + e_2 + e_3)(1 + z)$. Again, the matrix $M := \xi(g)$ shows that g is semi-reduced and basic and thus $\mathcal{C} = \mathfrak{p}^{-1}(\langle g \rangle)$ is a 3-dimensional σ -CCC with all Forney indices being 1. In this case, [9, Prop. 4.1] tells us that, if $n \geq 6$, the Griesmer bound for these parameters is given by the number $2(n - 2) + 1$. In the same way as above one can show that the codes just constructed have distance $2(n - 2)$, that is, they fail the Griesmer bound by 1. Proceeding in the same way for arbitrary $k \leq \frac{n}{2}$, one obtains k -dimensional unit memory σ -CCC's having distance $2(n - k + 1)$ which is $k - 2$ below the corresponding Griesmer bound.

Example 4.4 Let $q = 5$ and $n = 4$ and \bar{g} be as in Example 3.12. Write $\mathbb{F} = \mathbb{F}_5$. One easily checks that the matrix $\bar{M} = \xi(\bar{g})$ given in (3.19) is in $\mathcal{M}_{\text{basic}}$. Thus, the submodule $\mathcal{C} = \mathfrak{p}^{-1}(\langle \bar{g} \rangle) \subseteq \mathbb{F}[z]^4$ is a 3-dimensional σ -CCC with Forney indices 1, 1, 2. In order to compute a minimal encoder $G \in \mathbb{F}[z]^{3 \times 4}$ of \mathcal{C} we will apply Theorem 3.5(4). From \bar{g} as given in Example 3.12 we obtain the components $\bar{g}^{(1)} = 2e_1 + ze_2$, $\bar{g}^{(2)} = e_2 + 3ze_3$, $\bar{g}^{(3)} = e_3 + ze_4 + 4z^2e_1$. Identifying $f \in \mathbb{F}[x]/\langle x^4 - 1 \rangle$ with $[f(1), f(2), f(4), f(3)] \in A$ and using the map \mathfrak{p} from (2.4) we arrive at the minimal encoder matrix

$$G = \begin{pmatrix} \mathfrak{p}^{-1}(\bar{g}^{(1)}) \\ \mathfrak{p}^{-1}(\bar{g}^{(2)}) \\ \mathfrak{p}^{-1}(\bar{g}^{(3)}) \end{pmatrix} = \begin{pmatrix} 4z + 3 & 2z + 3 & z + 3 & 3z + 3 \\ 2z + 4 & 3z + 2 & 2z + 1 & 3z + 3 \\ z^2 + 4z + 4 & z^2 + 3z + 1 & z^2 + z + 4 & z^2 + 2z + 1 \end{pmatrix}.$$

Using some computer algebra routine one checks that this code attains the Griesmer bound (see [6, Eq. (1.3)]). Precisely, its distance is 6, which is the largest distance possible for any 3-dimensional code of length 4 over \mathbb{F}_5 with the same Forney indices.

Let us now turn to the existence of σ -CCC's with prescribed algebraic parameters. Corollary 4.2 raises the question whether for all $1 \leq k \leq n - 1$ and $\nu_1, \dots, \nu_k \in \mathbb{N}_0$ there exists a k -dimensional σ -CCC in $\mathbb{F}[z]^n$ with Forney indices ν_1, \dots, ν_k . The rest of this section will be devoted to this problem. We will start with showing that this problem can be split into two subproblems one of which is purely combinatorial.

Put

$$\hat{D} := \begin{pmatrix} 0 & 1 & 2 & \dots & n-2 & n-1 \\ n-1 & 0 & 1 & \dots & n-3 & n-2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 2 & 3 & 4 & \dots & 0 & 1 \\ 1 & 2 & 3 & \dots & n-1 & 0 \end{pmatrix}, \quad (4.2)$$

thus,

$$\hat{D}_{ab} = \begin{cases} b - a, & \text{if } b \geq a \\ n + b - a, & \text{if } b < a. \end{cases} = b - a \bmod n. \quad (4.3)$$

The role of the matrix \hat{D} is explained by the fact that for every matrix $M = (m_{ab}) \in \mathcal{M}$ we have

$$\mathcal{D}(M)_{ab} = \begin{cases} n \deg m_{ab} + \hat{D}_{ab} & \text{if } b \geq a, \\ n(\deg m_{ab} - 1) + \hat{D}_{ab} & \text{if } b < a. \end{cases} \quad (4.4)$$

The combinatorial problem we need to consider shows some close resemblance with the classical rook problem.

Problem 4.5 (Modified Rook Problem) *Let r_1, \dots, r_k be any (not necessarily different) numbers in $\{0, \dots, n-1\}$. Can we find these numbers in the matrix \hat{D} such that they appear in pairwise different rows and pairwise different columns? In other words, can we find distinct numbers i_1, \dots, i_k and distinct numbers j_1, \dots, j_k , all in the set $\{1, \dots, n\}$, such that*

$$\hat{D}_{i_l, j_l} = r_l \text{ for } l = 1, \dots, k. \quad (4.5)$$

The following slight reformulation will come handy for our purposes.

Remark 4.6 If Problem 4.5 is solvable for r_1, \dots, r_k then we can find these numbers even in the first $n-1$ rows of the matrix \hat{D} . In other words, (4.5) is true for some distinct numbers $i_1, \dots, i_k \in \{1, \dots, n-1\}$ and distinct numbers $j_1, \dots, j_k \in \{1, \dots, n\}$. Indeed, suppose we have a solution to 4.5, that is, $\hat{D}_{i_l, j_l} = r_l$ for $l = 1, \dots, k$. Then we may construct a second solution as follows. There exists some $\alpha \in \{1, \dots, n\}$ such that $i_l \neq \alpha$ for all l . Put $a_l = (i_l - \alpha - 1 \bmod n) + 1$ and $b_l = (j_l - \alpha - 1 \bmod n) + 1$. Since the numbers $(i_1 \bmod n), \dots, (i_k \bmod n)$ are pairwise different the same is true for a_1, \dots, a_k . Likewise b_1, \dots, b_k are pairwise different. Of course, $a_l, b_l \in \{1, \dots, n\}$ for all $l = 1, \dots, k$. Moreover, by construction $a_l \neq n$ for all $l = 1, \dots, k$, and upon using (4.3) we obtain $\hat{D}_{a_l, b_l} = b_l - a_l \bmod n = j_l - i_l \bmod n = \hat{D}_{i_l, j_l} = r_l$ for $l = 1, \dots, k$.

In the next section we will study Problem 4.5 in some more detail. Even though we are not able to provide a proof of the solvability for general numbers r_1, \dots, r_k we will consider some special cases where we present a complete proof. We would like to express our strong belief that the problem can be solved for all given data r_1, \dots, r_{n-1} . This has been underscored by a routine check with Maple confirming our conjecture for all $n \leq 10$.

The second problem we need to consider has an affirmative answer and thus can be stated as a theorem. The proof will be presented at the end of this section.

Theorem 4.7 *Let $j_1, \dots, j_{n-1} \in \{1, \dots, n\}$ be pairwise different and $d_1, \dots, d_{n-1} \in \mathbb{N}_0$ be such that*

$$j_i < i \implies d_i > 0. \quad (4.6)$$

Then there exists a basic matrix $M = (m_{ij}) \in \mathbb{F}[t]^{(n-1) \times n}$ with the following properties:

(i) $\deg m_{ij} \leq d_i$ for $j < j_i$,

- (ii) $\deg m_{ij} = d_i$ for $j = j_i$,
- (iii) $\deg m_{ij} < d_i$ for $j > j_i$,
- (iv) $m_{ii}(0) = 1$ for all i ,
- (v) $m_{ij}(0) = 0$ for $j < i$.

Notice that the properties (i) – (iii) simply tell us that the i -th row degree is given by d_i and the rightmost entry with degree d_i is in column j_i . Moreover, observe that without (4.6) the requirements (ii) and (v) would not be compatible. Using Proposition 3.10 we see that if we extend M by a zero row at the bottom we obtain a semi-reduced matrix in $\mathcal{M}_{\text{basic}}$.

Now we can show the following.

Theorem 4.8 *Let $1 \leq k \leq n - 1$ and $\nu_1, \dots, \nu_k \in \mathbb{N}_0$. Put $r_l = \nu_l \bmod n$ for $l = 1, \dots, k$. If Problem 4.5 is solvable for r_1, \dots, r_k then there exists a k -dimensional σ -CCC in $\mathbb{F}[z]^n$ with Forney indices ν_1, \dots, ν_k .*

As a consequence, if Problem 4.5 is solvable for all $r_1, \dots, r_{n-1} \in \{0, \dots, n - 1\}$ then for all $1 \leq k \leq n - 1$ and all $\nu_1, \dots, \nu_k \in \mathbb{N}_0$ there exists a k -dimensional σ -CCC in $\mathbb{F}[z]^n$ with Forney indices ν_1, \dots, ν_k .

PROOF: Let $k \in \{1, \dots, n - 1\}$ and $\nu_1, \dots, \nu_k \in \mathbb{N}_0$. Write $\nu_l = \hat{d}_l n + r_l$, where $\hat{d}_l \in \mathbb{N}_0$ and $0 \leq r_l \leq n - 1$. By assumption and Remark 4.6 there exist distinct $i_1, \dots, i_k \in \{1, \dots, n - 1\}$ and distinct $j_1, \dots, j_k \in \{1, \dots, n\}$ such that $\hat{D}_{i_l, j_l} = r_l$ for $l = 1, \dots, k$. Pick $1 \leq i_{k+1}, \dots, i_{n-1} \leq n - 1$ and $1 \leq j_{k+1}, \dots, j_{n-1} \leq n$ such that i_1, \dots, i_{n-1} as well as j_1, \dots, j_{n-1} are pairwise different. Define $r_l := \hat{D}_{i_l, j_l}$ for $l = k + 1, \dots, n - 1$ and put $\hat{d}_l := 0$ and $\nu_l := r_l$ for $l = k + 1, \dots, n - 1$. Now we re-index the numbers r_1, \dots, r_{n-1} in order to obtain

$$\hat{D}_{l, j_l} = r_l \text{ for } l = 1, \dots, n - 1. \quad (4.7)$$

Define

$$d_l := \begin{cases} \hat{d}_l & \text{if } j_l \geq l, \\ \hat{d}_l + 1 & \text{if } j_l < l. \end{cases} \quad (4.8)$$

Then (4.6) is true and Theorem 4.7 guarantees the existence of a matrix $\tilde{M} = (m_{ij}) \in \mathbb{F}[t]^{(n-1) \times n}$ satisfying (i) – (v). Extending \tilde{M} by a zero row at the bottom results in a semi-reduced matrix $M \in \mathcal{M}_{\text{basic}}$, see also Proposition 3.10(4). Using (4.4), we see that the maxima in the first $n - 1$ rows of $\mathcal{D}(M)$ are given by

$$\mathcal{D}(M)_{l, j_l} = \begin{cases} nd_l + \hat{D}_{l, j_l} = n\hat{d}_l + r_l = \nu_l, & \text{if } j_l \geq l, \\ n(d_l - 1) + \hat{D}_{l, j_l} = n\hat{d}_l + r_l = \nu_l, & \text{if } j_l < l. \end{cases}$$

Finally, deleting the rows of M corresponding to the $n - 1 - k$ artificially added indices $\nu_{k+1}, \dots, \nu_{n-1}$ (in the original ordering) we obtain a semi-reduced matrix $N \in \mathcal{M}_{\text{basic}}$, and Corollary 4.2 shows that $\mathfrak{p}^{-1}(\bullet(\xi^{-1}(N)))$ is a k -dimensional code with Forney indices ν_1, \dots, ν_k . \square

Example 4.9 Suppose we want a 3-dimensional σ -CCC $\mathcal{C} \subseteq \mathbb{F}_5[z]^4$ with Forney indices 4, 3, 3. Thus, $q = 5$ and $n = 4$. The remainders modulo n of the desired Forney indices

are 0, 3, 3, and by inspection we find $\hat{D}_{1,4} = 3 =: r_1$, $\hat{D}_{2,1} = 3 =: r_2$, $\hat{D}_{3,3} = 0 =: r_3$. Thus, (4.7) is true for $(j_1, j_2, j_3) = (4, 1, 3)$. This gives us the ordering $\nu_1 = 3, \nu_2 = 3, \nu_3 = 4$ of the Forney indices, and we have $\hat{d}_1 = \hat{d}_2 = 0$ and $\hat{d}_3 = 1$. Following (4.8) we put $d_1 = 0, d_2 = 1, d_3 = 1$. Then we have all data for Theorem 4.7. One easily sees that the matrix

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 \\ t & 1 & 0 & 0 \\ 0 & 0 & 1+t & 1 \end{pmatrix}$$

is basic and satisfies (i) – (v) of that theorem. Adding a zero row at the bottom gives us a semi-reduced matrix $N \in \mathcal{M}_{\text{basic}}$, and using Corollary 4.2 we see that $\mathcal{C} = \mathfrak{p}^{-1}(\langle \xi^{-1}(N) \rangle)$ is a 3-dimensional σ -CCC in $\mathbb{F}_5[z]^4$ with Forney indices 3, 3, 4. An encoder matrix of \mathcal{C} can be obtained as follows. The rows of M along with the isomorphism ξ result in the component polynomials $g^{(1)} = e_1 + z^3e_4$, $g^{(2)} = e_2 + z^3e_1$, $g^{(3)} = e_3 + ze_4 + z^4e_3$. Using the same identification of A with $\mathbb{F}_5[z]/\langle x^4 - 1 \rangle$ as in Example 4.4 we obtain from Theorem 3.5(4) that

$$G = \begin{pmatrix} \mathfrak{p}^{-1}(g^{(1)}) \\ \mathfrak{p}^{-1}(g^{(2)}) \\ \mathfrak{p}^{-1}(g^{(3)}) \end{pmatrix} = \begin{pmatrix} 4z^3 + 4 & 3z^3 + 4 & z^3 + 4 & 2z^3 + 4 \\ 4z^3 + 4 & 4z^3 + 2 & 4z^3 + 1 & 4z^3 + 3 \\ 4z^4 + 4z + 4 & z^4 + 3z + 1 & 4z^4 + z + 4 & z^4 + 2z + 1 \end{pmatrix}$$

is a minimal encoder of \mathcal{C} . It should be pointed out that the distance of this code is far from being optimal. This is due to the abundance of zeros in the matrix M causing many zero coefficients in the matrix G .

Let us briefly mention the following converse of Theorem 4.8. Indeed, it is easy to see that the existence of $(n-1)$ -dimensional σ -CCC's with arbitrarily prescribed Forney indices implies the solvability of Problem 4.5 for any given numbers $r_1, \dots, r_{n-1} \in \{0, \dots, n-1\}$. In more detail, the existence of such codes implies the existence of semi-reduced polynomials $g \in A[z; \sigma]$ with support satisfying $|T_g| = n-1$ and arbitrarily given degrees of its nonzero components. Using Proposition 3.10(3) this shows the solvability of Problem 4.5 for $k = n-1$, and thus for arbitrary $k \in \{1, \dots, n-1\}$.

While the general formulation of Theorem 4.8 is based on the assumption that we can solve Problem 4.5 we have some specific cases with fully established existence results.

Theorem 4.10 *Let $1 \leq k \leq \frac{n+1}{2}$. Then for all $\nu_1, \dots, \nu_k \in \mathbb{N}_0$ there exists a k -dimensional σ -CCC having Forney indices ν_1, \dots, ν_k .*

PROOF: Using Theorem 4.8 it suffices to show that Problem 4.5 can be solved for any given numbers $r_1, \dots, r_k \in \{0, \dots, n-1\}$ if $k \leq \frac{n+1}{2}$. First of all, it is clear that there exists j_1 such that $\hat{D}_{1,j_1} = r_1$, and we will proceed by induction. Thus, let us assume that we found distinct indices i_1, \dots, i_{k-1} and j_1, \dots, j_{k-1} such that $\hat{D}_{i_l, j_l} = r_l$ for $l = 1, \dots, k-1$. After a suitable permutation of the rows and columns of \hat{D} we obtain a matrix

$$\tilde{D} = \begin{pmatrix} \tilde{D}_1 & \tilde{D}_2 \\ \tilde{D}_3 & \tilde{D}_4 \end{pmatrix} \text{ where } \tilde{D}_1 = \text{diag}(r_1, \dots, r_{k-1}) \in \mathbb{Z}^{(k-1) \times (k-1)}$$

and where the other matrices are of fitting sizes. In particular, the matrix \tilde{D}_3 is of size $(n-k+1) \times (k-1)$. Since the entries of each row (resp. column) of \tilde{D} are pairwise different and, by assumption, $n-k+1 > k-1$ there exists at least one row of \tilde{D}_3 that does not contain the entry r_k . But then r_k must occur in the submatrix \tilde{D}_4 , and therefore we have found r_1, \dots, r_k in the matrix \hat{D} in pairwise different columns and rows. \square

One might wonder whether the last result can be extended to codes with arbitrary dimension by using dual codes. Recall that the dual \mathcal{C}^\perp of a k -dimensional code $\mathcal{C} \subseteq \mathbb{F}[z]^n$ has dimension $n-k$. However, it is a well-known fact in convolutional coding theory that the Forney indices of the dual code are not determined by the Forney indices of the given code. This is also true in the special case of σ -CCC's as one can easily see by some examples. As a consequence, Theorem 4.10 does not imply any existence results for codes with higher dimension.

In the next section we will show that we can solve Problem 4.5 for parameters r_1, \dots, r_{n-1} that attain at most two different values, see Proposition 5.2. Consequently, we have the following result.

Theorem 4.11 *Let $1 \leq k \leq n-1$ and $\nu_1, \dots, \nu_k \in \mathbb{N}_0$. If $|\{\nu_1 \bmod n, \dots, \nu_k \bmod n\}| \leq 2$ then there exists a k -dimensional σ -CCC in $\mathbb{F}[z]^n$ with Forney indices ν_1, \dots, ν_k .*

We will close this section with the

PROOF OF THEOREM 4.7:

We assume that \mathbb{F} is any finite field and $n \geq 2$. The following notation will be helpful. For a matrix $A \in \mathbb{F}[t]^{n \times (n+1)}$ and $l = 1, \dots, n+1$ let $A^{(l)}$ denote the n -minor of A obtained by omitting column l . Recall that A is basic if and only if the polynomials $A^{(1)}, \dots, A^{(n+1)}$ are coprime.

We will prove even more than stated in Theorem 4.7. We will show that for the given data there exists a matrix M satisfying the requirements of the theorem and with the following additional properties:

(vi) The only nonzero elements below the diagonal of M are at the positions (i, j_i) where $j_i < i$ and they are of the form t^{d_i} . This, of course, implies (v).

(vii) If $j_i < i$, then the only nonconstant element in the i -th row is at position (i, j_i) .

Using (vi), part (vii) tells us that if $j_i < i$ then all elements at positions (i, j) where $j \geq i$ are constant.

We will proceed by induction on n . Let $n = 2$ and j_1, d_1 be given. For $j_1 = 1$ the matrices $M = (1 + t^{d_1}, 1)$, if $d_1 > 0$, and $M = (1, 0)$, if $d_1 = 0$, are basic and have the properties (i) – (vii). If $j_1 = 2$, the matrix $M = (1, t^{d_1})$ satisfies all requirements.

Let now $n \geq 2$ and assume that for all possible j_1, \dots, j_{n-1} and $d_1, \dots, d_{n-1} \in \mathbb{N}_0$ a basic matrix $M \in \mathbb{F}[t]^{(n-1) \times n}$ satisfying (i) – (vii) exists. Throughout this proof we will call such a matrix a solution for the parameters $(j_1, \dots, j_{n-1}; d_1, \dots, d_{n-1})$. Notice that due to (iv) and (v) we have $t \nmid M^{(n)}$.

Assume now we have pairwise different indices $j_1, \dots, j_n \in \{1, \dots, n+1\}$ and integers $d_1, \dots, d_n \in \mathbb{N}_0$ such that (4.6) holds true. We will show the existence of a basic matrix $M \in \mathbb{F}[t]^{n \times (n+1)}$ satisfying (i) – (vii) separately for each of the following cases.

Case 1: $j_n = n + 1$. Then $j_1, \dots, j_{n-1} \leq n$ and by induction hypothesis there exists a solution $\hat{M} = (\hat{m}_1, \dots, \hat{m}_n) \in \mathbb{F}[t]^{(n-1) \times n}$ for the parameters $(j_1, \dots, j_{n-1}; d_1, \dots, d_{n-1})$. Put

$$M = \left(\begin{array}{cccc|c} \hat{m}_1 & \cdots & \hat{m}_{n-1} & \hat{m}_n & 0 \\ 0 & \cdots & 0 & 1 & t^{d_n} \end{array} \right) \in \mathbb{F}[t]^{n \times (n+1)}.$$

Since $M_{n,n} = 1$ and \hat{M} satisfies (i) – (vii) the same is true for M . Moreover, M is basic as we can see by considering the n -minors. Indeed, we have $M^{(i)} = \pm t^{d_n} \hat{M}^{(i)}$ for $i = 1, \dots, n$ and $M^{(n+1)} = \pm \hat{M}^{(n)}$. Now the coprimeness of $M^{(1)}, \dots, M^{(n+1)}$ follows from the basicness of \hat{M} along with the fact that $t \nmid \hat{M}^{(n)}$.

Case 2: $j_n = n$ and $d_n = 0$. For $i = 1, \dots, n - 1$ put

$$\hat{j}_i = \begin{cases} j_i & \text{if } j_i < n \\ n & \text{if } j_i = n + 1 \end{cases}$$

(notice that the case $j_i = n + 1$ need not occur). Then the indices $(\hat{j}_1, \dots, \hat{j}_{n-1}; d_1, \dots, d_{n-1})$ satisfy (4.6) and thus there exists a solution $\hat{M} = (\hat{m}_1, \dots, \hat{m}_n) \in \mathbb{F}[t]^{(n-1) \times n}$ for these parameters. Put

$$M = \left(\begin{array}{cccc|c} \hat{m}_1 & \cdots & \hat{m}_{n-1} & 0 & \hat{m}_n \\ 0 & \cdots & 0 & 1 & 0 \end{array} \right) \in \mathbb{F}[t]^{n \times (n+1)}.$$

It is easy to see that M is a solution for $(j_1, \dots, j_n; d_1, \dots, d_n)$.

Case 3: $j_n = n$ and $d_n > 0$. Choose \hat{M} as in the previous case and put

$$M = \left(\begin{array}{cccc|c} \hat{m}_1 & \cdots & \hat{m}_{n-1} & \hat{m}_n & \hat{m}_n \\ 0 & \cdots & 0 & 1 + t^{d_n} & 1 \end{array} \right) \in \mathbb{F}[t]^{n \times (n+1)}.$$

In this case the n -minors of M are given by $M^{(n+1)} = \pm(1 + t^{d_n})\hat{M}^{(n)}$ and $M^{(n)} = \pm\hat{M}^{(n)}$, whereas for $i = 1, \dots, n - 1$ we have by expansion along the last row $M^{(i)} = \pm((1 + t^{d_n})\hat{M}^{(i)} - \hat{M}^{(i)}) = \pm t^{d_n} \hat{M}^{(i)}$. Again, basicness of \hat{M} along with the fact that $t \nmid \hat{M}^{(n)}$ implies basicness of M . It is easy to see that M satisfies the properties (i) – (vii).

Case 4: $j_n =: \alpha < n$. Then $d_n > 0$. We have to distinguish further cases.

(a) If $j_i \leq n$ for all $i = 1, \dots, n - 1$ let $\hat{M} = (\hat{m}_1, \dots, \hat{m}_n)$ be a solution for the parameters $(j_1, \dots, j_{n-1}; d_1, \dots, d_{n-1})$ and put

$$M = \left(\begin{array}{ccccc|c} \hat{m}_1 & \cdots & \hat{m}_\alpha & \cdots & \hat{m}_n & 0 \\ & & t^{d_n} & & 1 & 1 \end{array} \right) \in \mathbb{F}[t]^{n \times (n+1)}.$$

It is easy to see that M is basic and satisfies (i) – (vii).

(b) Suppose now there exists some index β such that $j_\beta = n + 1$ and assume that $\beta \leq \alpha$. Then we may proceed as follows. For $i = 1, \dots, n - 1$ put

$$\hat{j}_i = \begin{cases} j_i & \text{if } i \neq \beta \\ \alpha & \text{if } i = \beta \end{cases}$$

Then $\hat{j}_1, \dots, \hat{j}_{n-1}$ are pairwise different and $(\hat{j}_1, \dots, \hat{j}_{n-1}; d_1, \dots, d_{n-1})$ satisfy (4.6). Thus by induction hypothesis there exists a solution $\hat{M} = (\hat{m}_1, \dots, \hat{m}_n) \in \mathbb{F}[t]^{(n-1) \times n}$ for the parameters $(\hat{j}_1, \dots, \hat{j}_{n-1}; d_1, \dots, d_{n-1})$. Put

$$M = \left(\begin{array}{cccc|c} \hat{m}_1 & \cdots & \hat{m}_\alpha & \cdots & \hat{m}_n \\ & & t^{d_n} & & 1 \\ & & & & 0 \end{array} \right) \in \mathbb{F}[t]^{n \times (n+1)},$$

where for $j \in \{1, \dots, n-1\} \setminus \{\alpha\}$ a zero entry occurs at the position (n, j) . This matrix does not yet satisfy (i) – (vii), and we will take care of it later on. Let us first show that M is basic. Computing the n -minors we obtain $M^{(n+1)} = \pm t^{d_n} \hat{M}^{(\alpha)} \pm \hat{M}^{(n)}$ and $M^{(\alpha)} = \pm \hat{M}^{(n)}$ whereas for $i \notin \{\alpha, n+1\}$ we have $M^{(i)} = \pm t^{d_n} \hat{M}^{(i)}$ (since the cofactor of the entry 1 in the last row is zero). Hence again $t \nmid \hat{M}^{(n)}$ together with the basicness of \hat{M} implies the basicness of M . Let us now turn to the properties (i) – (vii). First of all it is easy to see that $M = (m_{ij})$ satisfies (i), (ii), (iv), and (v). In particular, in the row β , where $j_\beta = n+1$, we have by construction $\deg m_{\beta, n+1} = d_\beta$ as well as $\deg m_{\beta, j} \leq d_\beta$ for $j < n+1$. Furthermore, properties (vi) and (vii) are satisfied since they are true for \hat{M} along with the facts that $\beta \leq \alpha$ and $j_\beta = n+1 > \beta$. Thus, let us turn to (iii). By construction property (iii) is satisfied for those indices i for which $j_i < \alpha$. The only obstacle occurs when $j_i > \alpha$. In this case we also have $\deg m_{ij} < d_i$ for $j_i < j < n+1$, but the entry in the last column does not necessarily satisfy this degree constraint. Due to property (iii) for \hat{M} we have instead $\deg m_{i, n+1} \leq d_i$ if $j_i \geq \alpha$. We will now perform elementary column operations in order to meet this final degree constraint. These column operations will only change the last column of M and do not destroy any of the properties mentioned above. For $l = \alpha+1, \dots, n$ we consecutively perform the following steps. If there exists an index i_0 such that $j_{i_0} = l$ and $\deg m_{i_0, n+1} = d_{i_0}$ then we add a suitable constant multiple of the l -th column of M to the last column such that the resulting entry at position $(i_0, n+1)$ has degree strictly less than d_{i_0} . This is possible since $\deg m_{i_0, j_{i_0}} = d_{i_0}$. Now the resulting matrix satisfies (iii) for all indices i such that $j_i \leq l$. Moreover, all other degree constraints remain valid. In particular, in the row β for which $j_\beta = n+1$ we still have $\deg m_{\beta, n+1} = d_\beta$. This way we finally obtain a solution for the parameters $(j_1, \dots, j_n; d_1, \dots, d_n)$.

(c) It remains to consider the case where there exists some index $\beta > \alpha$ such that $j_\beta = n+1$. Notice that $\beta < n$. For $i = 1, \dots, n-1$ put

$$(\hat{j}_i, \hat{d}_i) = \begin{cases} (j_i, d_i) & \text{if } i \neq \beta \\ (\alpha, d_n + d_\beta) & \text{if } i = \beta \end{cases}$$

Then $\hat{j}_1, \dots, \hat{j}_{n-1}$ are pairwise different and $(\hat{j}_1, \dots, \hat{j}_{n-1}; \hat{d}_1, \dots, \hat{d}_{n-1})$ satisfies (4.6) since $\hat{d}_\beta = d_n + d_\beta \geq d_n > 0$. Thus, by induction hypothesis there is a solution $\hat{M} = (\hat{m}_1, \dots, \hat{m}_n) \in \mathbb{F}[t]^{(n-1) \times n}$ for the parameters $(\hat{j}_1, \dots, \hat{j}_{n-1}; \hat{d}_1, \dots, \hat{d}_{n-1})$. Put

$$M = \left(\begin{array}{cccc|c} \hat{m}_1 & \cdots & \hat{m}_\alpha & \cdots & \hat{m}_n \\ & & t^{d_n} & & 0 \\ & & & & 1 \end{array} \right) \in \mathbb{F}[t]^{n \times (n+1)},$$

where for $i \in \{1, \dots, n-1\} \setminus \{\alpha\}$ a zero entry occurs at the position (n, i) . The n -minors of M are given by $M^{(n+1)} = \pm \hat{M}^{(n)} \pm t^{d_n} \hat{M}^{(\alpha)}$ and $M^{(n)} = \pm \hat{M}^{(n)}$, whereas for $i < n$ we have $M^{(i)} = \pm \hat{M}^{(i)}$. Thus M is basic. Furthermore, properties (i) – (vii) are satisfied

for all rows with index $i \neq \beta$, and only the β -th row needs to be adjusted. Since \hat{M} satisfies (iv), (vi), and (vii) the β -th row and the n -th row of M are given by

$$(0, \dots, 0, t^{d_n+d_\beta}, 0, \dots, 0, f_\beta, f_{\beta+1}, \dots, f_n, 0), \text{ for some } f_l \in \mathbb{F},$$

$$(0, \dots, 0, t^{d_n}, 0, \dots, 0, 0, 0, \dots, 1, 1),$$

respectively, where the entries $t^{d_n+d_\beta}$ and t^{d_n} appear in the α -th position, and the entry f_β is in the β -th position. Moreover, $f_\beta = 1$ by (iv). Now we see that we may subtract t^{d_β} times the n -th row of M from the β -th row in order to obtain a new matrix M' where the β -th row is of the form

$$(0, \dots, 0, 0, f_\beta, f_{\beta+1}, \dots, f_n - t^{d_\beta}, -t^{d_\beta}),$$

where still the entry f_β is in the β -th position. Since $j_\beta = n + 1$ now properties (i) – (vii) are satisfied for $i = \beta$, whereas the other rows did not change. This finally shows that M' satisfies all requirements (i) – (vii). \square

5 The Modified Rook Problem

In this short section we will briefly discuss Problem 4.5 for $k := n - 1$ given numbers. First of all, notice that the matrix \hat{D} in (4.2) is the addition table of the group $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ if the elements are ordered suitably. This has actually been used implicitly in Remark 4.6. The additive group \mathbb{Z}_n allows us to reformulate the problem. In order to do so let

$$\mathcal{P} := \{(x_1, \dots, x_{n-1}) \in \mathbb{Z}_n^{n-1} \mid x_1, \dots, x_{n-1} \text{ are pairwise different}\}$$

and

$$\mathcal{S} := \{r \in \mathbb{Z}_n^{n-1} \mid \exists x, y \in \mathcal{P} : r = x + y\}.$$

As a consequence, Problem 4.5 is solvable for all $r \in \mathbb{Z}_n^{n-1}$ if and only if $\mathcal{S} = \mathbb{Z}_n^{n-1}$. Here are some simple properties of the set \mathcal{S} .

Proposition 5.1

- (i) $\gamma \mathbf{1} \in \mathcal{S}$ for all $\gamma \in \mathbb{Z}_n$.
- (ii) If $r \in \mathcal{S}$, then $\tau(r) \in \mathcal{S}$ for all permutations τ in the symmetric group S_{n-1} .
- (iii) If $r \in \mathcal{S}$, then $\gamma r \in \mathcal{S}$ for all $\gamma \in \mathbb{Z}_n^\times$.
- (iv) If $r \in \mathcal{S}$, then $r + \gamma \mathbf{1} \in \mathcal{S}$ for all $\gamma \in \mathbb{Z}_n$.
- (v) $\mathcal{P} \subseteq \mathcal{S}$.

PROOF: Properties (i), (ii) and (iii) are obvious, whereas (iv) follows from the fact that if $x \in \mathcal{P}$ then $x + \gamma \mathbf{1} \in \mathcal{P}$ for all $\gamma \in \mathbb{Z}_n$. Let us now turn to (v). If $r \in \mathcal{P}$, then the entries of r attain $n - 1$ of the n different elements in \mathbb{Z}_n . Using (ii) we may assume that $r = (0, 1, \dots, \alpha - 1, \alpha + 1, \dots, n - 1)$ for some $\alpha \in \mathbb{Z}_n$. Again by (ii) we have $r \in \mathcal{S} \iff r' := (\alpha + 1, \dots, n - 1, 0, 1, \dots, \alpha - 1) \in \mathcal{S}$. By (iv) this in turn is equivalent

to $s := r' - \alpha \mathbf{1} = (1, 2, \dots, n-1) \in \mathcal{S}$. Hence it suffices to show that $s \in \mathcal{S}$. For n being odd one has $s + x = y$ where

$$x = (2, 3, \dots, \frac{n-1}{2}, \frac{n+1}{2}, \frac{n+3}{2}, \dots, n-1, 0), \quad y = (3, 5, \dots, n-2, 0, 2, \dots, n-3, n-1).$$

Since n is odd x, y are in \mathcal{P} which shows that $s \in \mathcal{S}$. For n even one has $s + x = y$ where

$$\begin{aligned} x &= \left(\frac{n}{2}, \frac{n}{2} + 1, \dots, n-2, n-1, 1, \dots, \frac{n}{2} - 2, \frac{n}{2} - 1 \right), \\ y &= \left(\frac{n}{2} + 1, \frac{n}{2} + 3, \dots, \frac{n}{2} + n-3, \frac{n}{2} + n-1, \frac{n}{2} + 2, \dots, \frac{n}{2} + n-4, \frac{n}{2} + n-2 \right) \end{aligned}$$

Again, $x, y \in \mathcal{P}$, showing the desired result. \square

Proposition 5.2 *If $r = (r_1, \dots, r_{n-1}) \in \mathbb{Z}_n^{n-1}$ has at most two different entries, that is, $|\{r_1, \dots, r_{n-1}\}| \leq 2$, then $r \in \mathcal{S}$.*

PROOF: If $r_1 = \dots = r_{n-1}$, then the assertion is in Proposition 5.1(i). Otherwise, using Proposition 5.1(ii) we may assume $r = (\alpha, \dots, \alpha, \beta, \dots, \beta)$ for some $\alpha \neq \beta$. Using part(iv) of that proposition we may even assume that $\alpha = 0$. Thus, let

$$r = (\underbrace{0, \dots, 0}_{n-1-f}, \underbrace{\beta, \dots, \beta}_f) \text{ for some } 1 \leq f \leq n-2.$$

In order to prove $r \in \mathcal{S}$ let l be the additive order of β in \mathbb{Z}_n and put

$$t := (t_1, \dots, t_n) := (0, \beta, \dots, (l-1)\beta, 1, 1+\beta, \dots, 1+(l-1)\beta, \dots, \beta-1, 2\beta-1, \dots, l\beta-1).$$

That is, the entries of t are sorted according to the group $\langle \beta \rangle$ and its cosets. Now put

$$\begin{aligned} x &= (t_1, \dots, t_{n-f-1}, t_{n-f+1}, \dots, t_n), \\ y &= (-t_1, \dots, -t_{n-f-1}, \beta - t_{n-f+1}, \dots, \beta - t_n). \end{aligned}$$

Then $r = x + y$ and, obviously, $x \in \mathcal{P}$. In order to see that $y \in \mathcal{P}$ notice first that the first $n-f-1$ entries are obviously pairwise different, and so are the last f entries. Assume now $\beta - t_j = -t_i$ for some $n-f+1 \leq j \leq n$ and $1 \leq i \leq n-f-1$. Then $t_j = \beta + t_i$. But by construction $\beta + t_i = t_{i+1}$ if $i \notin l\mathbb{Z}$ and $\beta + t_i = t_{(m-1)l+1}$ if $i = ml$. Since $j > n-f > i$ this shows that $\beta + t_i \neq t_j$. Hence $y \in \mathcal{P}$ and thus $r \in \mathcal{S}$. \square

Notice that the vector t above could also be defined according to a different ordering of the cosets of $\langle \beta \rangle$. This shows, that there are many ways of writing $r = x + y$ for some $x, y \in \mathcal{P}$.

Unfortunately, we are not aware of any way to generalize the last proof to vectors $r \in \mathbb{Z}_n^{n-1}$ with 3 or more different entries.

6 Extension to General Automorphisms — An Example

So far we have studied σ -CCC's in $\mathbb{F}[z]^n$ where $n \mid (q-1)$ and where the automorphism σ induces a cycle of length n on the primitive idempotents of A . In this section we will

briefly illustrate how the results can be utilized for general automorphisms if $n \mid (q-1)$. For ease of notation let us restrict to the following example.

Let $q = 8$ and $n = 7$. Consider the automorphism $\sigma \in \text{Aut}_{\mathbb{F}}(A)$ defined by

$$\sigma(e_1) = e_2, \sigma(e_2) = e_3, \sigma(e_3) = e_1, \sigma(e_4) = e_5, \sigma(e_5) = e_6, \sigma(e_6) = e_7, \sigma(e_7) = e_4.$$

In cycle notation this reads as $(e_1, e_2, e_3)(e_4, e_5, e_6, e_7)$. Define $A_1 := \mathbb{F} \times \mathbb{F} \times \mathbb{F}$ and $A_2 := \mathbb{F} \times \mathbb{F} \times \mathbb{F} \times \mathbb{F}$ and denote the primitive idempotents of A_1 (resp. A_2) simply by e_1, e_2, e_3 (resp. e_4, e_5, e_6, e_7). Then it is straightforward to establish the isomorphism

$$A[z; \sigma] \longmapsto A_1[z; \sigma_1] \times A_2[z; \sigma_2], \quad g \longmapsto \left(g^{(1)} + g^{(2)} + g^{(3)}, g^{(4)} + g^{(5)} + g^{(6)} + g^{(7)} \right), \quad (6.1)$$

where for $i = 1, 2$ the automorphism σ_i on A_i is defined by the cycle (e_1, e_2, e_3) and (e_4, e_5, e_6, e_7) , respectively. Furthermore, a polynomial in $A[z; \sigma]$ is (semi-)reduced if and only if each factor in $A_i[z; \sigma_i]$ is (semi-)reduced. As a consequence, the investigation of left ideals and direct summands in $A[z; \sigma]$ amounts to the study of the same type of objects in the rings $A_i[z; \sigma_i]$. Since for these rings the automorphism induces a cycle of maximal length on the primitive idempotents this brings us to the situation of the previous sections. Notice, however, that for the ring $A_1[z; \sigma_1]$ the length $n_1 := 3$ is not a divisor of $q-1$, and thus, $A_1 \not\cong \mathbb{F}[x]/\langle x^3 - 1 \rangle$. In Remark 3.15 we mentioned that one can prove the results of Section 3 in this case as well with the only exception of Theorem 3.5(4) which does not make sense anymore. Along with the isomorphism (6.1) this is sufficient in order to construct CCC's for this automorphism as well. Let us illustrate this idea by an example.

Example 6.1 Let $\alpha \in \mathbb{F}_8$ be the primitive element satisfying the identity $\alpha^3 + \alpha + 1 = 0$. For $i = 1, 2$ let $\xi_i : A_i[z; \sigma_i] \longrightarrow \mathcal{M}_i$ be the isomorphism with the according matrix ring as introduced in Proposition 3.2. The matrices

$$M_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & \alpha^4 \\ 0 & 0 & 0 \end{pmatrix} \in \mathcal{M}_1 \text{ and } M_2 = \begin{pmatrix} \alpha^6 & 1 & \alpha & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^3 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in \mathcal{M}_2$$

are obviously basic and semi-reduced, and thus so are the polynomials $g_1 = \xi_1^{-1}(M_1) = e_2 + z\alpha^4 e_3 \in A_1[z; \sigma_1]$ and $g_2 = \xi_2^{-1}(M_2) = \alpha^6 e_4 + \alpha^3 e_6 + z(e_5 + e_7) + z^2 \alpha e_6 \in A_2[z; \sigma_2]$. Using the isomorphism in (6.1) we obtain the semi-reduced and basic polynomial $g = g_1 + g_2 = e_2 + \alpha^6 e_4 + \alpha^3 e_6 + z(\alpha^4 e_3 + e_5 + e_7) + z^2 \alpha e_6 \in A[z; \sigma]$. Its support is given by $T_g = \{2, 4, 6\}$. As a consequence, $\langle g \rangle$ is a direct summand of rank 3 of the left $\mathbb{F}[z]$ -module $A[z; \sigma]$. Now [8, Thm. 7.13(b)] (which is also valid for semi-reduced polynomials) tells us that the matrix

$$G := \begin{pmatrix} \mathfrak{p}^{-1}(g^{(2)}) \\ \mathfrak{p}^{-1}(g^{(4)}) \\ \mathfrak{p}^{-1}(g^{(6)}) \end{pmatrix} \in \mathbb{F}[z]^{3 \times 7}$$

is a minimal encoder for the σ -CCC $\mathcal{C} := \mathfrak{p}^{-1}(\langle g \rangle) \subseteq \mathbb{F}[z]^7$. By construction, the code has Forney indices 1, 2, 1. Of course, basicness and minimality of the matrix G can also be checked directly once the rows of the matrix have been computed using the mapping \mathfrak{p} from (2.4). Using a computer algebra routine one finds that the distance of \mathcal{C} is 12. In other words, the code attains the Griesmer bound, see [6, Eq. (1.3)].

Concluding Remarks

In this paper we studied a particular class of CCC's. We showed that the existence of such codes with any given algebraic parameters can be reduced to solving a certain combinatorial problem. Under the assumption this problem is solvable for all possible instances this shows that the class of σ -CCC's is, in a certain sense, as rich as the class of all CC's. We strongly believe that the combinatorial problem is solvable for all instances, but that has to remain open for future research. Moreover, the potential of our approach needs to be further exploited with respect to error-correcting properties. With the exception of the codes in Example 4.3 the considerations so far do not result in classes of codes having provably large distance.

References

- [1] J. A. Domínguez Pérez, J. M. Muñoz Porras, and G. Serrano Sotelo. Convolutional codes of Goppa type. *Appl. Algebra Engrg. Comm. and Comput.*, 15:51–61, 2004.
- [2] S. Estrada, J. R. García Rozas, J. Peralta, and E. Sánchez García. Group convolutional codes. 2007. Available at <http://front.math.ucdavis.edu/> with ID-number RA/0702543v1.
- [3] G. D. Forney Jr. Convolutional codes I: Algebraic structure. *IEEE Trans. Inform. Theory*, IT-16:720–738, 1970. (see also corrections in *IEEE Trans. Inf. Theory*, vol. 17, 1971, p. 360).
- [4] G. D. Forney Jr. Minimal bases of rational vector spaces, with applications to multivariable linear systems. *SIAM J. on Contr.*, 13:493–520, 1975.
- [5] H. Gluesing-Luerssen and B. Langfeld. A class of one-dimensional MDS convolutional codes. *J. Algebra Appl.*, 5:505–520, 2006.
- [6] H. Gluesing-Luerssen and B. Langfeld. On the algebraic parameters of convolutional codes with cyclic structure. *J. Algebra Appl.*, 5:53–76, 2006.
- [7] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache. Strongly MDS convolutional codes. *IEEE Trans. Inform. Theory*, 52:584–598, 2006.
- [8] H. Gluesing-Luerssen and W. Schmale. On cyclic convolutional codes. *Acta Applicandae Mathematicae*, 82:183–237, 2004.
- [9] H. Gluesing-Luerssen and W. Schmale. On doubly-cyclic convolutional codes. *Appl. Algebra Engrg. Comm. Comput.*, 17:151–170, 2006.
- [10] R. Hutchinson, J. Rosenthal, and R. Smarandache. Convolutional codes with maximum distance profile. *Syst. Contr. Lett.*, 54:53–63, 2005.
- [11] A. V. Jategaonkar. Skew polynomial rings over semisimple rings. *J. Algebra*, 19:315–328, 1971.

- [12] R. Johannesson and K. S. Zigangirov. *Fundamentals of Convolutional Coding*. IEEE Press, New York, 1999.
- [13] J. Justesen. Algebraic construction of rate $1/\nu$ convolutional codes. *IEEE Trans. Inform. Theory*, IT-21:577–580, 1975.
- [14] J. L. Massey, D. J. Costello, and J. Justesen. Polynomial weights and code constructions. *IEEE Trans. Inform. Theory*, IT-19:101–110, 1973.
- [15] J. L. Massey and M. K. Sain. Codes, automata, and continuous systems: Explicit interconnections. *IEEE Trans. Aut. Contr.*, AC-12:644–650, 1967.
- [16] R. J. McEliece. The algebraic theory of convolutional codes. In V. Pless and W. Huffman, editors, *Handbook of Coding Theory, Vol. 1*, pages 1065–1138. Elsevier, Amsterdam, 1998.
- [17] J. M. Muñoz Porras, J. A. Domínguez Pérez, J. I. I. Curto, and G. Serrano Sotelo. Convolutional Goppa codes. *IEEE Trans. Inform. Theory*, 52:340–344, 2006.
- [18] P. Piret. Structure and constructions of cyclic convolutional codes. *IEEE Trans. Inform. Theory*, IT-22:147–155, 1976.
- [19] P. Piret. *Convolutional Codes; An Algebraic Approach*. MIT Press, Cambridge, MA, 1988.
- [20] C. Roos. On the structure of convolutional and cyclic convolutional codes. *IEEE Trans. Inform. Theory*, IT-25:676–683, 1979.
- [21] J. Rosenthal, J. M. Schumacher, and E. V. York. On behaviors and convolutional codes. *IEEE Trans. Inform. Theory*, IT-42:1881–1891, 1996.
- [22] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Appl. Algebra Engrg. Comm. Comput.*, 10:15–32, 1999.
- [23] J. Rosenthal and E. V. York. BCH convolutional codes. *IEEE Trans. Inform. Theory*, IT-45:1833–1844, 1999.
- [24] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Constructions of MDS-convolutional codes. *IEEE Trans. Inform. Theory*, IT-47:2045–2049, 2001.